

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-022216

(43)Date of publication of application : 24.01.2003

(51)Int.Cl.

G06F 12/14

B42D 15/10

G06K 19/07

(21)Application number : 2001-207210

(71)Applicant : HITACHI LTD

(22)Date of filing : 09.07.2001

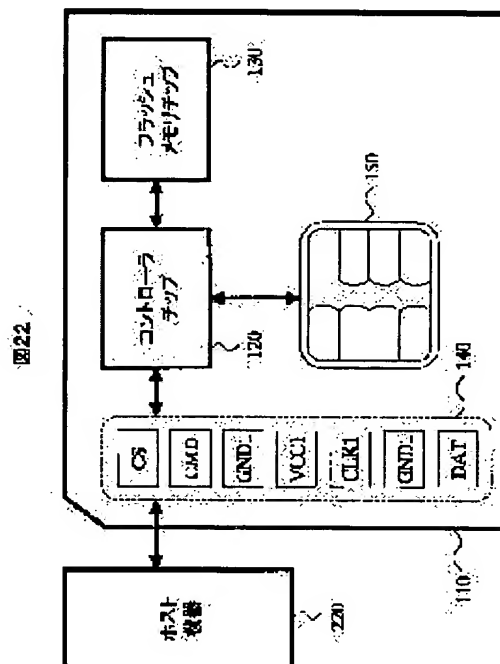
(72)Inventor : HATANO TOMIHISA  
TODA AKINORI  
TSUNODA MOTOYASU  
MIZUSHIMA EIGA  
KATAYAMA KUNIHIRO

## (54) STORAGE DEVICE

### (57)Abstract:

PROBLEM TO BE SOLVED: To realize the high speed processing of a multi-media card.

SOLUTION: This storage device is provided with a flash memory chip 130, an IC card chip 150 capable of executing security processing (encryption or decoding or the like), and a controller chip 120 for controlling the reading/ writing of data for the flash memory chip and the IC card chip. Moreover, the controller chip 120 simultaneously accesses the flash memory chip 130 and the IC card chip 150 in response to a request from a host.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-22216

(P 2 0 0 3 - 2 2 2 1 6 A)

(43) 公開日 平成15年1月24日 (2003.1.24)

(51) Int. Cl. <sup>7</sup>	識別記号	F I	ターマコード (参考)	
G06F 12/14	320	G06F 12/14	320	B 2C005
	310		310	K 5B017
B42D 15/10	501	B42D 15/10	501	B 5B035
	521		521	
G06K 19/07		G06K 19/00		N
		審査請求 未請求 請求項の数 8	O L	(全36頁)

(21) 出願番号 特願2001-207210 (P 2001-207210)

(22) 出願日 平成13年7月9日 (2001.7.9)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 幡野 富久

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 戸田 昭憲

神奈川県横浜市戸塚区吉田町292番地 株

式会社日立マイクロソフトウェアシステム

ズ内

(74) 代理人 100075096

弁理士 作田 康夫

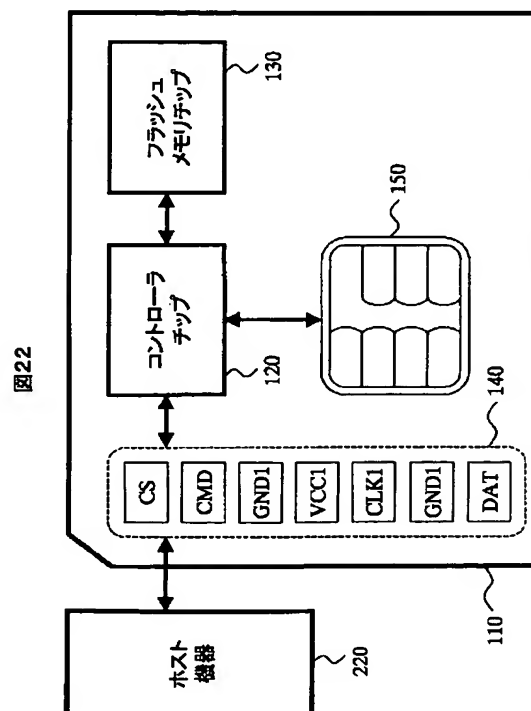
最終頁に続く

(54) 【発明の名称】 記憶装置

(57) 【要約】

【課題】 本発明は、マルチメディアカードの処理の高速化を図ることを目的とする。

【解決手段】 本発明は、フラッシュメモリチップ130と、セキュリティ処理（暗号化や復号化等）を実行可能なICカードチップ150と、ホストからの要求に応じて、フラッシュメモリチップ及びICカードチップへのデータの読み書きを制御するコントローラチップ120とを備える。さらに、コントローラチップ120は、フラッシュメモリチップ130とICカードチップ150の両方にホストからの要求に応じて同時にアクセスする。



## 【特許請求の範囲】

【請求項 1】データを記憶するための記憶装置において、前記データを記憶可能な第 1 のメモリと、前記データを記憶可能でかつ前記データのセキュリティ処理を実行可能な第 2 のメモリと、ホスト機器からのコマンドに基づいて、前記第 1 のメモリ又は前記第 2 のメモリを選択するコントローラとを有し、

前記ホスト機器から前記第 1 のメモリへのアクセスを実行している間に前記第 2 のメモリに対する前記ホスト機器からの第 2 のコマンドを受け付け、前記第 2 のコマンドに従う処理を実行することを特徴とする記憶装置。

【請求項 2】前記コントローラは、前記ホスト機器からのコマンドに前記データのセキュリティ処理に関する情報が含まれていた場合に、前記第 2 のメモリを選択する請求項 1 に記載の記憶装置。

【請求項 3】前記第 2 のメモリは、セキュリティ評価機関によって予め認証された IC チップであることを特徴とする請求項 1 に記載の記憶装置。

【請求項 4】前記認証済 IC チップは、該認証済 IC チップへ読み書きされるデータを暗号化又は復号化する手段を有することを特徴とする請求項 3 に記載の記憶装置。

【請求項 5】前記第 1 のメモリは、前記ホスト機器からのデータを記憶する第 1 の記憶領域と、前記第 2 のメモリに関するデータを記憶し、前記ホスト機器からのデータの読み出し又は書き込みの少なくとも 1 つが制限される第 2 の記憶領域とを有することを特徴とする請求項 4 に記載の記憶装置。

【請求項 6】前記コントローラは、前記第 2 の記憶領域に記憶されたデータを、前記第 2 のメモリへ転送する手段を有することを特徴とする請求項 5 に記載の記憶装置。

【請求項 7】前記コントローラは、前記第 2 の記憶領域に記憶されたデータに基づいて、前記第 2 のメモリを制御することを特徴とする請求項 6 に記載の記憶装置。

【請求項 8】コンテンツプロバイダによって発行されたセッション鍵によって暗号化された第一及び第二のコンテンツを記憶するメモリと、前記コンテンツプロバイダによって公開鍵によって暗号化されたセッション鍵と前記公開鍵に対応する秘密鍵とを記憶し、前記秘密鍵によって前記セッション鍵を復号化することが可能なメモリ付演算処理装置と、ホストからのコマンドに応じて、前記メモリ付演算処理装置に前記第一のコンテンツに対応する前記セッション鍵の復号化させながら、既に復号化された前記第二のコンテンツに対応する前記セッション鍵によって前記メモリに記憶された前記第二のコンテンツを復号化し、復号化された前記コンテンツを前記ホストへ送信するコントローラとを備えた記憶装置。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、セキュリティ機能を搭載した記憶装置、その記憶装置が挿入可能なホスト機器、及びその記憶装置が挿入されたホスト機器に係り、特に、フラッシュメモリチップ及びコントローラを有するメモリカード及びそのメモリカードが挿入可能な装置及びそのメモリカードが挿入された端末装置に関する。

【0002】

【従来の技術】IC カードは、プラスチックカード基板中に IC（集積回路）チップを埋め込んだものであり、その表面に IC チップの外部端子を持つ。IC チップの外部端子には、電源端子、クロック端子、データ入出力端子などが含まれる。IC チップは、接続装置が外部端子から電源や駆動クロックを直接供給することによって動作する。

【0003】IC カードは、外部端子を通して端末機などの接続装置との間で電気信号を送受信することにより、接続装置と情報交換をおこなう。情報交換の結果として、IC カードは計算結果や記憶情報の送出、記憶情報の変更をおこなう。IC カードは、これらの動作仕様に基いて、機密データ保護や個人認証などのセキュリティ処理を実行する機能を持つことができる。IC カードは、クレジット決済やバンキングなど機密情報のセキュリティが必要とされるシステムにおいて、個人識別のためのユーザデバイスとして利用されている。

【0004】

【発明が解決しようとする課題】セキュリティシステムにおいて利用される IC カードは、IC カード内部で秘密情報を用いて演算を行う際に、その秘密情報あるいはその秘密情報を推定できるような情報を IC カードの外部にももらさないように設計される必要がある。すなわち、耐タンパ性を持つことが必要とされる。このような外部にももらしてはならない秘密情報を解析する攻撃方法としては、タイミング解析、電力差分析、故障利用解析などが知られている。

【0005】タイミング解析は、暗号処理時間が秘密情報の内容に依存して異なる場合、その時間差を統計的に解析して秘密情報を推定する攻撃法である。暗号アルゴリズムを装置に実装する際、暗号の処理時間の短縮やプログラムサイズの縮小を目的として、秘密情報の内容に依存して不要となる処理をスキップしたり分岐処理を行ったりするような最適化が行われることがある。このような最適化を行った場合、暗号処理時間が秘密情報の内容に依存して異なる。そのため、処理時間を見ることで秘密情報の内容を推定できる可能性がある。

【0006】電力差分析は、暗号処理を実行している最中に、IC カードの電源端子から供給される電力を測定し、そこから消費電力の差分を解析することにより秘密情報を推定する攻撃法である。

50 【0007】故障利用解析は、IC カードの計算誤りを

利用した攻撃法である。ICカードに一過性の故障あるいは他の機能に影響を与えない範囲の限定的な障害を与え、ICカードに攻撃者の望む異常な処理を行わせる。例えば、ICカードに高電圧を加えたり、瞬間的にクロック周波数や駆動電圧を変動させることにより故意にエラーを発生させた場合に得られる誤った計算結果と正しい計算結果から秘密情報が取得される可能性がある。

【0008】したがって、ICカードは、実用上、これらの攻撃法に対する対策手段を持たなければならない。

【0009】本発明の目的は、セキュリティを向上した記憶装置を提供することにある。

【0010】

【課題を解決するための手段】上記課題を解決するため、本発明は、データを記憶するための記憶装置において、データを記憶可能な第1のメモリと、データを記憶可能でかつデータのセキュリティ処理を実行可能な第2のメモリと、ホスト機器からのコマンドに基づいて、第1のメモリ又は第2のメモリを選択するコントローラと有し、ホスト機器から第1のメモリへのアクセスを実行している間に第2のメモリに対するホストからの第2のコマンドを受け付け、第2のコマンドに従う処理を実行する構成とする。

【0011】又、コントローラは、ホスト機器からのコマンドにデータのセキュリティ処理に関する情報が含まれていた場合に、第2のメモリを選択する構成でも良い。

【0012】さらに、第2のメモリは、セキュリティ評価機関によって予め認証されたICチップであることも考えられる。

【0013】また、認証済ICチップは、認証済ICチップへ読み書きされるデータを暗号化又は復号化する手段を有する。

【0014】また、第1のメモリは、ホスト機器からのデータを記憶する第1の記憶領域と、第2のメモリに関するデータを記憶し、ホスト機器からのデータの読み出し又は書き込みの少なくとも1つが制限される第2の記憶領域とを有する構成とすることもできる。

【0015】さらに、コントローラは、第2の記憶領域に記憶されたデータを、第2のメモリへ転送する手段を有することもできる。

【0016】また、コントローラは、第2の記憶領域に記憶されたデータに基づいて、第2のメモリを制御する構成を有しても良い。

【0017】さらに、本発明の実施形態として、コンテンツプロバイダによって発行されたセッション鍵によって暗号化された第一及び第二のコンテンツを記憶するメモリと、コンテンツプロバイダによって公開鍵によって暗号化されたセッション鍵と公開鍵に対応する秘密鍵とを記憶し、秘密鍵によってセッション鍵を復号化することが可能なメモリ付演算処理装置と、ホスト機器からの

コマンドに応じて、メモリ付演算処理装置に第一のコンテンツに対応するセッション鍵の復号化させながら、既に復号化された第二のコンテンツに対応するセッション鍵によってメモリに記憶された第二のコンテンツを復号化し、復号化された第二のコンテンツをホスト機器へ送信するコントローラとを有する構成とする。

【0018】

【発明の実施の形態】図22は、本発明を適用したMultiMediaCard (MultiMediaCardは、Infineon Technologies AGの登録商標である。以下、「MMC」と略記する。)の内部構成を示した図である。MMC110は、MMC仕様に準拠するのが好ましい。MMC110は、MMC110に接続されたホスト機器220から発行されたMMC仕様に準拠したメモリカードコマンドに基づいて、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。

【0019】ホスト機器220は、例えば、携帯電話、携帯情報端末(PDA)、パーソナルコンピュータ、音楽再生(及び録音)装置、カメラ、ビデオカメラ、自動預金預払器、街角端末、及び決済端末等が該当する。

【0020】MMC110は、MMC外部端子140、コントローラチップ120、フラッシュメモリチップ130、及びICカードチップ150を持つ。フラッシュメモリチップ130は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。MMC外部端子140は、外部のホスト機器220と情報交換するために、電源供給端子、クロック入力端子、コマンド入出力端子、データ入出力端子、グランド端子等の7つの端子から構成される。コントローラチップ120は、MMC外部端子140、フラッシュメモリチップ130、及びICカードチップ150と接続され、これらを制御するマイコンチップである。

【0021】ICカードチップ150は、ICカードのプラスチック基板中に埋め込むためのマイコンチップであり、ICカードチップ150が有する外部端子、電気信号プロトコル、コマンドはISO/IEC7816規格に準拠している。ICカードチップ150の外部端子には、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子、及びグランド端子がある。コントローラチップ120は、ICカードチップ150の外部端子からICカードチップ150にICカードコマンドを発行することによって、外部のホスト機器220から要求されたセキュリティ処理に必要な演算をおこなう。

【0022】図26は、本発明のICカードチップの内部構成を示す図である。ICカードチップ150は、演算処理を行うためのCPU(マイコン)158、データ(プログラムを含む。)を記憶するためのROM(Read

Only Memory) 159、RAM (Random Access Memory) 160、EEPROM (Electrically Erasable Programmable ROM) 162、暗号／復号に間する処理を行うための暗号コプロセッサ163、及び外部とデータを送受信するためのシリアルインターフェース161とを備える。これらはバス164によって相互に接続される。

【0023】暗号コプロセッサ163は、ホスト機器220からのコマンドに応じて、セキュリティ処理を実行する。尚、暗号コプロセッサ163（ハードウェア）の代わりに、プログラム（ソフトウェア）を用いてCPU158がセキュリティ処理を実行してもよい。セキュリティ処理は、例えば、ICカードチップ150内の記憶領域にデータが書き込まれるとき、又は、ICカードチップ150内の記憶領域からデータが読み出されるときに実行される。

【0024】フラッシュメモリチップ130は、不揮発性の記憶素子を有する。一般的に、ICカードチップ150のEEPROM162の記憶容量は、フラッシュメモリチップ130の記憶容量より小さい。但し、EEPROM162の記憶容量は、フラッシュメモリチップ130の記憶容量と同じでもよいし、大きくてもよい。

【0025】ICカードチップ150には、セキュリティ評価基準の国際標準であるISO/IEC15408の評価・認証機関によって認証済みである製品を利用するのが望ましい。一般に、セキュリティ処理をおこなう機能を持つICカードを実際の電子決済サービスなどで利用する場合、そのICカードはISO/IEC15408の評価・認証機関による評価と認定を受ける必要がある。MMCにセキュリティ処理をおこなう機能を追加することによってMMC110を実現し、それを実際の電子決済サービスなどで利用する場合、MMC110も同様にISO/IEC15408の評価・認証機関による評価と認定を受ける必要がある。本発明においては、MMC110は、評価・認証機関によって認証済みのICカードチップ150を内蔵し、そのICカードチップ150を利用してセキュリティ処理をおこなう構造を持つことにより、セキュリティ処理機能を得る。したがって、MMC110はISO/IEC15408に基づくセキュリティ評価基準を容易に満足することができ、MMCにセキュリティ処理機能を追加するための開発期間を短縮することができる。

【0026】MMC110は、MMC仕様に準拠した外部インタフェースを持つのが好ましい。MMC110は、一種類の外部インタフェースを通じて、標準メモリカードコマンド（フラッシュメモリチップ130へアクセスするためのコマンド）に加えて、セキュリティ処理を実行するコマンドを受け付ける必要がある。コントローラチップ120は、MMC110が受信したコマンドが標準メモリカードコマンドであるか、セキュリティ処

理を実行するコマンドであるかによって、アクセスすべきチップを選択し、コマンド処理を分配する機能を持つ。本実施形態においては、コントローラチップ120は、標準メモリカードコマンドを受信したならば、フラッシュメモリチップ130を選択し、これにフラッシュメモリコマンドを発行してホストデータを読み書きできる。また、セキュリティ処理を実行するコマンドを受信したならば、ICカードチップ150を選択し、これにICカードコマンドを発行してセキュリティ処理を実行することができる。

【0027】ICカードチップ150の外部端子は、グランド端子を除いて、電源供給端子、クロック入力端子、リセット入力端子、I/O入出力端子がコントローラチップ120と接続されている。

【0028】コントローラチップ120は、電源供給端子、クロック入力端子を通して、ICカードチップ150への電源供給、クロック供給を制御する。本実施形態によれば、ホスト機器220からセキュリティ処理を要求されないときには、コントローラチップ120がICカードチップ150への電源供給やクロック供給を停止することができ、MMC110の電力消費を削減することができる。

【0029】電源が供給されていないICカードチップ150を、ICカードコマンドを受信できる状態にするには、まず、ICカードチップ150に電源供給を開始し、リセット処理を施す必要がある。コントローラチップ120は、MMC110がホスト機器220からセキュリティ処理を実行するコマンドを受信したのを契機に、電源供給端子を通してICカードチップ150への電源供給を開始する機能を有する。また、コントローラチップ120は、MMC110がホスト機器220からセキュリティ処理を実行するコマンドを受信したのを契機に、リセット入力端子を通してICカードチップ150のリセット処理をおこなう機能を有する。本実施形態によれば、コントローラチップ120は、セキュリティ処理を実行するコマンドを受信するまでICカードチップ150への電源供給を停止させておくことができる。したがって、MMC110の電力消費を削減することができる。

【0030】コントローラチップ120は、ICカードチップ150のクロック入力端子を通してICカードチップ150に供給するクロック信号をMMC110内部で発生し、その周波数、供給開始タイミング、供給停止タイミングを制御する機能を有する。本実施形態によれば、MMC外部端子140のクロック入力端子のクロック信号と無関係にすることができるため、ホスト機器220によるタイミング解析、電力差分解析、故障利用解析と呼ばれる攻撃法に対してセキュリティが向上する。

【0031】図21は、フラッシュメモリチップ130の内部構成を示す図である。フラッシュメモリチップ1

30は、ホストデータ領域2115及び管理領域2110とを有する。ホストデータ領域2115は、セクタ単位に論理アドレスがマッピングされている領域であり、ホスト機器220が論理アドレスを指定してデータを読み書きできる領域である。

【0032】ホストデータ領域2115は、ユーザファイル領域2130及びセキュリティ処理アプリケーション領域2120とを有する。ユーザファイル領域2130は、ユーザが自由にファイルデータを読み書きできる領域である。セキュリティ処理アプリケーション領域2120は、ホスト機器220がセキュリティ処理アプリケーションに必要なデータを格納する領域であり、ユーザが不正にアクセスしないように、ホスト機器220のセキュリティ処理アプリケーションによって論理的にユーザアクセス制限がかけられる。ここに格納されるデータとしては、ホスト機器220のアプリケーションプログラム、そのアプリケーション専用のデータ、及びセキュリティ処理に使用される証明書など（例えば、電子決済アプリケーションプログラム、電子決済ログ情報、電子決済サービス証明書など）がある。本実施形態によれば、MMC110が、ホスト機器220がセキュリティ処理をおこなう上で使用するデータをホスト機器220の代わりに格納するため、ホスト機器220にとって利便性が向上する。

【0033】管理領域2110は、コントローラチップ120がICカードチップ150を管理するための情報を格納する領域である。管理領域2110は、ICカード制御パラメータ領域2111、ICカード環境設定情報領域2112、CLK2設定情報領域2113、セキュリティ処理バッファ領域2114、及びセキュリティ処理ステータス領域2116とを有する。2111～2116の領域の詳細な使用方法については後述する。

【0034】コントローラチップ120は、フラッシュメモリチップ130の管理領域2110のセキュリティ処理バッファ領域2114を、ICカードチップ150でセキュリティ処理を実行する際のメインメモリまたはバッファメモリとして利用する。ホスト機器220がセキュリティ処理を実行するコマンドによりMMC110にアクセスした際に、MMC110がホスト機器220からICカードチップ150に一度に送信できないほどの大きなサイズのセキュリティ関連データを受信したならば、コントローラチップ120は、フラッシュメモリチップ130へのアクセスを選択し、受信したデータを十分な容量を持つセキュリティ処理バッファ領域2114に一時的に格納する。ICカードチップ150に一度に送信できないほどのサイズとは、ICカードコマンドの許容データサイズ（例えば、255バイト又は256バイト）を超えるサイズである。そして、コントローラチップ120はそれをICカードチップ150に送信できるサイズのデータに分割し、分割データをフラッシュ

メモリチップ130から読み出し、段階的にICカードチップ150に送信する。つまり、分割されたデータの読み出し、書き込みを繰り返す。本実施形態によれば、ホスト機器220にとって、大きなサイズのセキュリティ関連データを扱うことができるので、セキュリティ処理の利便性が向上する。

【0035】セキュリティ処理バッファ領域2114を含む管理領域2110は、ホスト機器220が不正にアクセスしてセキュリティ処理を解析することができないように、コントローラチップ120により物理的にホストアクセス制限がかけられている。つまり、管理領域2110はホスト機器220が直接データを読み書きできない。本実施形態によれば、ホスト機器220がセキュリティ処理バッファ領域2114の内容を自由に読み出したり改ざんすることができないため、セキュリティ処理の信頼性や安全性が向上する。

【0036】図23は、MMC110を利用したセキュリティ処理の一例として、コンテンツ配信のセキュリティ処理を表した図である。コンテンツプロバイダ2310は、MMC110を所有するユーザにコンテンツ2314を販売する業者である。ホスト機器220は、この例では、コンテンツプロバイダ2310とネットワークなどを介して接続することができる端末機である。ユーザは、MMC110をホスト機器220に接続してコンテンツ2314を購入する。以下、その手順を説明する。

【0037】まず、ホスト機器220は、MMC110に、フラッシュメモリチップ130に格納されたユーザ証明書2321を読み出すコマンドを発行する。MMC110のコントローラチップ120は、フラッシュメモリチップ130のセキュリティ処理アプリケーション領域2120に格納されたユーザ証明書2321を読み出し、それをホスト機器220に送信する。ユーザ証明書2321を受信したホスト機器220は、それをコンテンツプロバイダ2310に送信する。コンテンツプロバイダ2310は、ユーザ証明書2321につけられたデジタル署名を検証する（2311）。検証が成功したならば、コンテンツプロバイダ2310は、乱数発生器によりセッション鍵を生成し（2312）、それをユーザ証明書2321から抽出したユーザ公開鍵によって暗号化する（2313）。さらに、コンテンツプロバイダ2310は、コンテンツ2314をセッション鍵によって暗号化する（2315）。コンテンツプロバイダ2310は、ステップ2313の結果をホスト機器220に送信する。

【0038】ホスト機器220は、ステップ2313の結果をユーザ秘密鍵2322によって復号するセキュリティ処理を要求するコマンドを、MMC110に発行する。コントローラチップ120は、ステップ2313の結果をユーザ秘密鍵2322によって復号するICカー

ドコマンドを、ICカードチップ150に発行する。ICカードチップ150は、ユーザ秘密鍵2322によってステップ2313の結果を復号して、セッション鍵を取得する(2323)。ホスト機器220は、この復号処理が成功したかを示す情報を出力させるコマンドをMMC110に発行する。コントローラチップ120は、ICカードチップ150の出力する復号結果(復号処理が成功したかを示すICカードレスポンス)をもとにしてホスト機器220の求める情報を構築する。そして、MMC110はその情報をホスト機器220に送信する。

【0039】次に、コンテンツプロバイダ2310は、ステップ2315の結果を、ホスト機器220に送信する。ホスト機器220は、ステップ2313の結果をセッション鍵(ステップ2323によって取得した鍵)によって復号するセキュリティ処理を要求するコマンドを、MMC110に発行する。コントローラチップ120は、ステップ2315の結果をセッション鍵によって復号するICカードコマンドを、ICカードチップ150に発行する。ICカードチップ150は、セッション鍵によってステップ2315の結果を復号して、コンテンツ2314を復元する(2324)。コントローラチップ120は、このコンテンツ2314をICカードチップ150から受信し、フラッシュメモリチップ130に書きこむ。ホスト機器220は、この復号処理が成功したかを示す情報を出力させるコマンドをMMC110に発行する。コントローラチップ120は、ICカードチップ150の出力する復号結果(復号処理が成功したかを示すICカードレスポンス)をもとにしてホスト機器220の求める情報を構築する。そして、MMC110はその情報をホスト機器220に送信する。ホスト機器220が、コンテンツを無事に受信したことをコンテンツプロバイダ2310に伝え、コンテンツプロバイダ2310はユーザ証明書に記載されたユーザにコンテンツ料金を課金する。ユーザは、ホスト機器220でMMC110内のフラッシュメモリチップ130に格納されたコンテンツ2314を読み出して利用することができる。また、フラッシュメモリチップ130の記憶媒体に大容量のフラッシュメモリを使用すれば、多くのコンテンツを購入できる。本実施形態によれば、コンテンツ配信におけるセキュリティ処理とコンテンツ蓄積の両方をMMC110によって容易に実現できる。コンテンツ料金の決済を、ICカードチップ150を利用して行ってもよい。

【0040】図24及び図25は、それぞれ、本発明をSDカード(幅24ミリメートル、長さ32ミリメートル、厚さ2.1ミリメートルで、9つの外部端子をもち、フラッシュメモリを搭載した小型メモリカードである。)及びメモリースティック(メモリースティックはソニー株式会社の登録商標である。)に適用したときの

内部構成を表した図である。

【0041】本発明を適用したSDカード2410は、SDカードコントローラチップ2420、フラッシュメモリチップ2430、SDカード外部端子2440、及びICカードチップ150とを有する。本発明を適用したメモリースティック2510は、メモリースティックコントローラチップ2520、フラッシュメモリチップ2530、メモリースティック外部端子2540、及びICカードチップ150とを有する。

【0042】フラッシュメモリチップ2430及び2530は、不揮発性の半導体メモリを記憶媒体とするメモリチップであり、フラッシュメモリコマンドによりデータの読み書きができる。SDカードコントローラチップ2420及びメモリースティックコントローラチップ2520は、それぞれSDカードとメモリースティック内の他の構成要素を制御するマイコンチップである。

【0043】SDカード外部端子2440は、端からData2端子2441、Data3端子2442、Com端子2443、Vss端子2444、Vdd端子2445、Clock端子2446、Vss端子2447、Data0端子2448、Data1端子2449の順で並ぶ9つの端子を有する。Vdd端子2445は電源供給端子、Vss端子2444及び2447はグランド端子、Data0端子2448、Data1端子2449、Data2端子2441及びData3端子2442はデータ入出力端子、Com端子2443はコマンド入出力端子、Clock端子2446はクロック入力端子である。SDカード2410は、外部に接続するSDカードホスト機器2460とのインタフェース仕様がMMC110と異なるものの、MMC外部端子140と非常に類似した外部端子を持ち、MMC110と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【0044】一方、メモリースティック外部端子2540は、端からGnd端子2541、BS端子2542、Vcc端子2543、予約端子Rsvを1つ飛ばしてDIO端子2544、INS端子2545、予約端子Rsvを1つ飛ばしてSCK端子2546、Vcc端子2547、Gnd端子2548の順で並ぶ10個の端子を有する。Vcc端子2543及び2547は電源供給端子、Gnd端子2541及び2548はグランド端子、DIO端子2544はコマンドおよびデータ入出力端子、SCK端子2546はクロック入力端子である。メモリースティック2510は、外部に接続するメモリースティックホスト機器2560とのインタフェース仕様がMMC110と異なるものの、MMC110と同様に外部からコマンドを発行することにより動作する特徴を持つため、本発明を適用することができる。

【0045】図1は、本発明を適用したMMC110の内部構成を表した図である。また、図2は、図1のMM



C110と接続したホスト機器220の構成とその接続状態を表した図である。ホスト機器220は、VCC1電源221、CLK1発振器222、ホストインタフェース223を持つ。

【0046】MMC110は、外部のホスト機器220と情報交換するためのMMC外部端子140を持つ。MMC外部端子140は、CS端子141、CMD端子142、GND1端子143及び146、VCC1端子144、CLK1端子145、DAT端子147の7つの端子を有する。MMC仕様は、MMC110の動作モードとしてMMCモードとSPIモードという2種類を規定しており、動作モードによってMMC外部端子140の使用法は異なる。本実施例ではMMCモードでの動作の場合について詳細に説明する。

【0047】VCC1端子144は、VCC1電源221と接続されており、ホスト機器220がMMC110に電力を供給するための電源端子である。GND1端子143および146は、VCC1電源221と接続されており、MMC110の電氣的なグランド端子である。GND1端子143とGND1端子146は、MMC110内部で電氣的に短絡されている。

【0048】CS端子141は、ホストインタフェース223に接続されており、SPIモードの動作において使用される入力端子である。ホスト機器220が、MMC110にSPIモードでアクセスするときには、CS端子141にLレベルを入力する。MMCモードの動作では、CS端子141を使用する必要はない。CMD端子142は、ホストインタフェース223に接続されており、ホスト機器220が、メモリカードインタフェース仕様に準拠したメモリカードコマンドをMMC110に送信したり、同仕様に準拠したメモリカードレスポンスをMMC110から受信するために使用する入出力端子である。DAT端子147は、ホストインタフェース223に接続されており、ホスト機器220が、メモリカードインタフェース仕様に準拠した形式の入力データをMMC110に送信したり、同仕様に準拠した形式の出力データをMMC110から受信するために使用する入出力端子である。

【0049】CLK1端子145は、CLK1発振器222に接続されており、CLK1発振器222が生成するクロック信号が入力される端子である。ホスト機器220が、CMD端子142を通してメモリカードコマンド、メモリカードレスポンスを送受信したり、DAT端子147を通してホストデータを送受信するときに、CLK1端子145にクロック信号が入力される。ホストインタフェース223には、CLK1発振器222からクロック信号が供給されており、メモリカードコマンド、メモリカードレスポンス、ホストデータは、CLK1発振器222が生成するクロック信号にビット単位で同期して、ホスト機器220とMMC110との間を転

送される。

【0050】MMC110は、コントローラチップ120を持つ。コントローラチップ120は、CPU121、フラッシュメモリI/F制御回路122、MMC I/F制御回路123、CLK0発振器124、VCC2生成器125、VCC2制御回路126、CLK2制御回路127、ICカードI/F制御回路128とを有する。これらの構成要素121~128は、ホスト機器220からVCC1端子144やGND1端子143、146を通して供給された電力により動作する。MMC I/F制御回路123は、CS端子141、CMD端子142、CLK1端子145、及びDAT端子147と接続されており、MMC110がそれらの端子を通してホスト機器220と情報交換するためのインタフェースを制御する論理回路である。

【0051】CPU121は、MMC I/F制御回路123と接続されており、MMC I/F制御回路123を制御する。MMC I/F制御回路123がCMD端子142を通してホスト機器220からメモリカードコマンドを受信すると、MMC I/F制御回路123は、そのコマンドの受信が成功したかどうかの結果をホスト機器220に伝えるためCMD端子142を通してホスト機器220にレスポンスを送信する。CPU121は、受信したメモリカードコマンドを解釈し、コマンド内容に応じた処理を実行する。また、そのコマンド内容に応じてホスト機器220とDAT端子147を通してデータの送受信をおこなう必要がある場合、CPU121は、MMC I/F制御回路123へのデータの送出、MMC I/F制御回路123からのデータの取得をおこなう。さらに、CPU121は、MMC I/F制御回路123とホスト機器220との間のデータ転送手続きも制御する。例えば、ホスト機器220から受信したデータの処理中に、ホスト機器220がMMC110への電源供給を停止することがないように、CPU121はDAT端子147にLレベルを出力させ、MMC110がビジー状態であることをホスト機器220に伝える。CLK0発振器124は、CPU121と接続され、CPU121を動作させる駆動クロックを供給する。

【0052】MMC110は、フラッシュメモリチップ130を有する。フラッシュメモリチップ130は、不揮発性の半導体メモリを記憶媒体とするメモリチップである。フラッシュメモリチップ130は、ホスト機器220からVCC1端子144やGND1端子143、146を通して供給された電力により動作する。フラッシュメモリチップ130は、外部からのフラッシュメモリコマンドに従って、入力されたデータを不揮発性の半導体メモリに格納するライト機能、また同メモリに格納されたデータを外部に出力するリード機能を持つ。フラッシュメモリI/F制御回路122は、フラッシュメモリチップ130にフラッシュメモリコマンドを発行した



り、そのコマンドで入出力するデータを転送するための論理回路である。CPU121は、フラッシュメモリI/F制御回路122を制御し、フラッシュメモリチップ130にデータのライト機能やリード機能を実行させる。ホスト機器220から受信したデータをフラッシュメモリチップ130にライトしたり、フラッシュメモリチップ130に格納されたデータをホスト機器220に送信する必要があるとき、CPU121は、フラッシュメモリI/F制御回路122とMMCI/F制御回路123の間のデータ転送を制御する。

【0053】MMC110は、ICカードチップ150を有する。ICカードチップ150は、ICカードの基板中に埋め込むことを目的として設計されたICチップであり、ICカードの外部端子規格に準拠した8つの外部端子を有する。このうち6つの端子は、ICカードの外部端子規格により使用法が割り付けられており、残りの2つは将来のための予備端子である。その6つの端子は、VCC2端子151、RST端子152、CLK2端子153、GND2端子155、VPP端子156、及びI/O端子157である。

【0054】ICカードチップ150のグランド端子は、MMC外部端子140のGND1（グランド端子）146に接続される。ICカードチップ150のVCC2端子（電源入力端子）151は、コントローラチップ120のVCC2制御回路126に接続される。ICカードチップ150のRST端子（リセット入力端子）152とI/O端子（データ入出力端子）157は、コントローラチップ120のICカードI/F制御回路128に接続される。ICカードチップ150のCLK2端子（クロック入力端子）153は、コントローラチップ120のCLK2制御回路127に接続される。

【0055】フラッシュメモリチップ130のVCC端子（電源入力端子）は、MMC外部端子140のVCC1144に接続される。フラッシュメモリチップ130のVSS端子（グランド端子）は、MMC外部端子140のGND1146に接続される。フラッシュメモリチップ130のI/O端子（データ入出力端子）とレディ/ビジー端子とチップイネーブル端子とアウトプットイネーブル端子とライトイネーブル端子とクロック端子とリセット端子とは、コントローラチップ120のフラッシュメモリIF制御回路122に接続される。

【0056】VCC2端子151は、ICカードチップ150に電力を供給するための電源端子である。VCC2制御回路126は、MOS-FET素子を用いたスイッチ回路によりVCC2端子151への電力の供給開始と供給停止を制御する回路である。VCC2生成器125はVCC2端子151に供給する電圧を発生し、それをVCC2制御回路126に供給する。ICカードの電気信号規格は、ICカードの動作クラスとして、クラスAとクラスBを規定している。VCC2端子151に供

給する標準電圧は、クラスAでは5V、クラスBでは3Vである。本発明はICカードチップ150の動作クラスによらず適用できるが、本実施例ではICカードチップ150がクラスBで動作する場合について詳細に説明する。

【0057】VPP端子156は、ICカードチップ150がクラスAで動作する時に、内部の不揮発性メモリにデータを書き込んだり消去したりするために使用される可変電圧を供給する端子であり、クラスBで動作する時には使用しない。GND2端子155は、ICカードチップ150の電気的なグランド端子であり、GND1端子143、146と短絡されている。VCC2制御回路126はCPU121と接続され、CPU121はVCC2端子151への電力供給の開始と停止を制御することができる。ICカードチップ150を使用しないときは、CPU121はVCC2端子151への電力供給を停止することができる。MMC110は、ICカードチップ150への電力供給を停止することにより、それが消費する電力を節約することができる。ただし、電力供給を停止すると、ICカードチップ150の内部状態は、ICカードチップ150内部の不揮発性メモリに記憶されたデータを除いて維持されない。

【0058】CLK2端子153は、ICカードチップ150にクロック信号を入力する端子である。CLK2制御回路127は、CLK2端子153にクロックを供給する回路である。CLK2制御回路127は、CLK0発振器124から供給されたクロック信号をもとにしてCLK2端子153に供給するクロック信号を生成する。CLK2制御回路127はCPU121と接続されており、CLK2端子153へのクロックの供給開始と供給停止をCPU121から制御することができる。ICカードチップ150は、自身内部に駆動クロック発振器をもたない。そのため、CLK2端子153から駆動クロックを供給することによって動作する。CLK2制御回路127が、CLK2端子153へのクロック供給を停止すると、ICカードチップ150の動作は停止するため、ICカードチップ150の消費電力を低下させることができる。この時、VCC2端子151への電力供給が保たれていれば、ICカードチップ150の内部状態は維持される。

【0059】ここで、CLK2端子153に供給するクロック信号の周波数をF2、CLK0発振器124から供給されたクロック信号の周波数をF0、PとQを正の整数とすると、CLK2制御回路127は、 $F2 = (P/Q) * F0$ の関係になるようなクロック信号を作成して、これをCLK2端子153に供給する。PとQの値はCPU121により設定できるようになっている。Pを大きく設定してF2を大きくすると、ICカードチップ150の内部処理をより高速に駆動できる。Qを大きく設定してF2を小さくすると、ICカードチップ15

0 の内部処理はより低速に駆動され、IC カードチップ 150 の消費電力を低下させることができる。IC カードチップ 150 の駆動クロック周波数は、IC カードチップ 150 が正しく動作できるような許容周波数範囲内に設定される必要がある。そのため、CLK2 制御回路 127 は、F2 の値がその許容周波数範囲を外れるような P と Q の値を設定させない特徴を持つ。

【0060】I/O 端子 157 は、IC カードチップ 150 に IC カードコマンドを入力したり、IC カードチップ 150 が IC カードレスポンスを出力するときに使用 10 する入出力端子である。IC カード I/F 制御回路 128 は、I/O 端子 157 と接続されており、I/O 端子 157 を通して IC カードコマンドの信号送信や IC カードレスポンスの信号受信をおこなう回路である。IC カード I/F 制御回路 128 は CPU121 に接続されており、CPU121 は、IC カード I/F 制御回路 128 による IC カードコマンドや IC カードレスポンスの送受信の手続きを制御したり、送信すべき IC カードコマンドデータを IC カード I/F 制御回路 128 に 20 設定したり、受信した IC カードレスポンスを IC カード I/F 制御回路 128 から取得する。IC カード I/F 制御回路 128 には CLK2 制御回路 127 からクロックが供給されており、IC カードコマンドや IC カードレスポンスは、CLK2 端子 153 に供給するクロック信号にビット単位で同期して、I/O 端子 157 を通して送受信される。また、RST 端子 152 は、IC カードチップ 150 をリセットするときにリセット信号を入力する端子である。IC カード I/F 制御回路 128 は、RST 端子 152 と接続されており、CPU121 の指示により IC カードチップ 150 にリセット信号を送ることができる。

【0061】IC カードチップ 150 は、IC カードの電気信号規格やコマンド規格に基づいて情報交換をおこなう。IC カードチップ 150 へのアクセスパターンは 4 種類であり、図 3～図 6 を用いて各パターンを説明する。図 3 は、CPU121 の指示により IC カードチップ 150 が非活性状態（電源が遮断されている状態）から起動して内部状態を初期化するプロセス（以下、コールドリセットと呼ぶ）において、IC カードチップ 150 の外部端子の信号波形をシンプルに表した図である。図 4 は、CPU121 の指示により IC カードチップ 150 が活性状態（電源が供給されている状態）で内部状態を初期化するプロセス（以下、ウォームリセットと呼ぶ）において、IC カードチップ 150 の外部端子の信号波形をシンプルに表した図である。図 5 は、CPU121 の指示により IC カードチップ 150 に IC カードコマンドを送信し IC カードチップ 150 から IC カードレスポンスを受信するプロセスにおいて、IC カードチップ 150 の外部端子の信号波形をシンプルに表した図である。図 6 は、CPU121 の指示により IC カード 50

ドチップ 150 を非活性状態にするプロセスにおいて、IC カードチップ 150 の外部端子の信号波形をシンプルに表した図である。図 3～図 6 において、時間の方向は左から右にとっており、上の行から下の行に向かって VCC2 端子 151、RST 端子 152、CLK2 端子 153、I/O 端子 157 で観測される信号を表す。また、破線はそれぞれの信号の基準（L レベル）を表す。

【0062】図 3 を参照して、IC カードチップ 150 のコールドリセット操作を説明する。まず、IC カード I/F 制御回路 128 は、RST 端子 152 を L レベルにする（301）。次に、VCC2 制御回路 126 は、VCC2 端子への電源供給を開始する（302）。次に、CLK2 制御回路 127 は CLK2 端子 153 へのクロック信号の供給を開始する（303）。次に、IC カード I/F 制御回路 128 は I/O 端子 157 を状態 Z（ブルアップされた状態）にする（304）。次に、IC カード I/F 制御回路 128 は RST 端子 152 を H レベルにする（305）。次に、IC カード I/F 制御回路 128 は I/O 端子 157 から出力されるリセット 20 応答の受信を開始する（306）。リセット応答の受信が終了したら、CLK2 制御回路 127 は CLK2 端子 153 へのクロック信号の供給を停止する（307）。これで、コールドリセットの操作が完了する。なお、ステップ 307 は消費電力を低下させるための工夫であり、省略してもよい。

【0063】図 4 を参照して、IC カードチップ 150 のウォームリセット操作を説明する。まず、CLK2 制御回路 127 は CLK2 端子 153 へのクロック信号の供給を開始する（401）。次に、IC カード I/F 制御回路 128 は RST 端子 152 を L レベルにする（402）。次に、IC カード I/F 制御回路 128 は I/O 端子 157 を状態 Z にする（403）。次に、IC カード I/F 制御回路 128 は RST 端子 152 を H レベルにする（404）。次に、IC カード I/F 制御回路 128 は I/O 端子 157 から出力されるリセット応答の受信を開始する（405）。リセット応答の受信が終了したら、CLK2 制御回路 127 は CLK2 端子 153 へのクロック信号の供給を停止する（406）。これで、ウォームリセットの操作が完了する。なお、ステップ 406 は消費電力を低下させるための工夫であり、省略してもよい。

【0064】図 5 を参照して、IC カードチップ 150 に IC カードコマンドを送信し IC カードチップ 150 から IC カードレスポンスを受信する操作を説明する。まず、CLK2 制御回路 127 は CLK2 端子 153 へのクロック信号の供給を開始する（501）。なお、クロックがすでに供給されている場合、ステップ 501 は不要である。次に、IC カード I/F 制御回路 128 は I/O 端子 157 にコマンドデータの送信を開始する（502）。コマンドデータの送信が終了したら、IC

カード I/F 制御回路 128 は I/O 端子 157 を状態 Z にする (503)。次に、IC カード I/F 制御回路 128 は I/O 端子 157 から出力されるレスポンスデータの受信を開始する (504)。レスポンスデータの受信が終了したら、CLK2 制御回路 127 は CLK2 端子 153 へのクロック信号の供給を停止する (505)。これで、IC カードコマンド送信と IC カードレスポンス受信の操作が完了する。なお、ステップ 505 は、消費電力を低下させるための工夫であり、省略してもよい。

【0065】図 6 を参照して、IC カードチップ 150 を非活性化する操作を説明する。まず、CLK2 制御回路 127 は CLK2 端子 153 を L レベルにする (601)。次に、IC カード I/F 制御回路 128 は RST 端子 152 を L レベルにする (602)。次に、IC カード I/F 制御回路 128 は I/O 端子 157 を L レベルにする (603)。最後に、VCC2 制御回路 126 は VCC2 端子への電源供給を停止する (604)。これで、非活性化の操作が完了する。

【0066】IC カードチップ 150 は、機密データ保護や個人認証などに必要な暗号演算をおこなうセキュリティ処理機能を持つ。IC カードチップ 150 は、CPU 121 との間で IC カードコマンドや IC カードレスポンスの送受信することにより情報交換をおこない、その結果として、計算の結果や記憶されている情報の送出、記憶されている情報の変更などをおこなう。CPU 121 は、IC カードチップ 150 を利用してセキュリティ処理を実行することができる。MMC 110 がホスト機器 220 から特定のメモリカードコマンドを受信すると、CPU 121 はそれを契機として、VCC2 制御回路 126 を通して IC カードチップ 150 への電源供給を制御したり、または CLK2 制御回路 127 を通して IC カードチップ 150 へのクロック供給を制御したり、または IC カード I/F 制御回路 128 を通して IC カードチップ 150 に IC カードコマンドを送信する。これにより、CPU 121 は、IC カードチップ 150 を利用して、ホスト機器 220 が要求するセキュリティ処理を実行する。CPU 121 は、特定のメモリカードコマンドの受信を契機に、IC カードチップ 150 に対する電源供給制御、クロック供給制御、IC カードコマンド送信、IC カードレスポンス受信を複数組み合わせることで操作することによって、セキュリティ処理を実行してもよい。また、CPU 121 は、ホスト機器 220 が MMC 110 へ電源供給を開始したのを契機として、セキュリティ処理を実行してもよい。セキュリティ処理の結果は、IC カードチップ 150 が出力する IC カードレスポンスをベースにして構成され、MMC 110 内に保持される。MMC 110 がホスト機器 220 から特定のメモリカードコマンドを受信すると、CPU 121 はそれを契機として、セキュリティ処理の結果をホスト

機器 220 に送信する。

【0067】図 7 は、ホスト機器 220 が MMC 110 にアクセスするときのフローチャートを表したものである。まず、ホスト機器 220 は MMC 110 を活性化するために VCC1 端子 144 に電源供給を開始する (701)。これを契機として、MMC 110 は、第 1 次 IC カード初期化処理を実行する (702)。第 1 次 IC カード初期化処理の詳細は後述する。次に、ホスト機器 220 は MMC 110 を初期化するために CMD 端子 142 を通して MMC 110 の初期化コマンドを送信する (703)。この初期化コマンドは MMC 仕様準拠のものであり、複数種類ある。ホスト機器 220 は、MMC 110 を初期化するために、複数の初期化コマンドを送信する場合がある。MMC 110 が初期化コマンドを受信すると、MMC 110 はそれを処理する (704)。これを契機として、MMC 110 は、第 2 次 IC カード初期化処理を実行する (705)。第 2 次 IC カード初期化処理の詳細は後述する。

【0068】ホスト機器 220 は、MMC 110 の初期化コマンドに対するメモリカードレスポンスを、CMD 端子 142 を通して受信し、そのメモリカードレスポンスの内容から MMC 110 の初期化が完了したかを判定する。未完了ならば、再び初期化コマンドの送信をおこなう (703)。MMC 110 の初期化が完了したならば、ホスト機器 220 は、MMC 仕様準拠した標準メモリカードコマンド (フラッシュメモリチップ 130 へアクセスするためのコマンド) や、上に述べたセキュリティ処理に関連した特定のメモリカードコマンド (IC カードチップ 150 へアクセスするためのコマンド) の送信を待機する状態に移る (707)。この待機状態では、ホスト機器 220 は標準メモリカードコマンドを送信することができる (708)。MMC 110 が標準メモリカードコマンドを受信したら、MMC 110 はそれを処理する (709)。処理が完了したら、ホスト機器 220 は、再び待機状態にもどる (707)。この待機状態では、ホスト機器 220 はセキュリティ処理要求ライトコマンドを送信することもできる (710)。セキュリティ処理要求ライトコマンドとは、上に述べたセキュリティ処理に関連した特定のメモリカードコマンドの 1 種であり、MMC 110 にセキュリティ処理を実行させるために処理要求を送信するメモリカードコマンドである。

【0069】MMC 110 がセキュリティ処理要求ライトコマンドを受信したら、CPU 121 は、要求されたセキュリティ処理の内容を解釈し、セキュリティ処理を IC カードコマンドの形式で記述する (711)。即ち、CPU 121 は、予め定められたルールに従って、ホスト機器 230 からの標準メモリカードコマンドを、IC カードチップ 150 が解釈可能な特定のメモリカードコマンドへ変換する。そして、その結果として得られ

た IC カード コマンド を IC カード チップ 150 に発行  
 するなどして、要求されたセキュリティ処理を実行する  
 (712)。処理が完了したら、ホスト機器 220 は、  
 再び待機状態にもどる (707)。この待機状態では、  
 ホスト機器 220 はセキュリティ処理結果リードコマ  
 ンドを送信することもできる (713)。セキュリティ処  
 理結果リードコマンドとは、上に述べたセキュリティ処  
 理に関連した特定のメモリカードコマンドの 1 種であ  
 り、MMC 110 によるセキュリティ処理の実行結果を  
 知るために処理結果を受信するメモリカードコマンドで  
 ある。

【0070】MMC 110 がセキュリティ処理結果リー  
 ドコマンドを受信したら、CPU 121 は、IC カード  
 チップ 150 から受信した IC カードレスポンスをベー  
 スに、ホスト機器 220 に送信すべきセキュリティ処理  
 結果を構築する (714)。そして、ホスト機器 220  
 は、MMC 110 からセキュリティ処理結果を受信す  
 る。受信が完了したら、ホスト機器 220 は、再び待機  
 状態にもどる (707)。なお、ステップ 714 は、ス  
 テップ 712 の中でおこなってもよい。

【0071】図 7 において、ステップ 702 およびス  
 テップ 705 で実行する第 1 次 IC カード初期化処理お  
 よび第 2 次 IC カード初期化処理は、MMC 110 内でセ  
 キュリティ処理を実行するのに備えて、CPU 121 が  
 IC カードチップ 150 に対してアクセスする処理であ  
 る。具体的には、IC カードチップ 150 の活性化や非  
 活性化、IC カードチップ 150 のリセット、IC カ  
 ードチップ 150 の環境設定を行う。環境設定とは、セ  
 キュリティ処理を実行するために必要な情報 (例えば、使  
 用可能な暗号アルゴリズムの情報、暗号計算に使用する  
 秘密鍵や公開鍵に関する情報、個人認証に使用する認証  
 データに関する情報など) を IC カードチップ 150 か  
 ら読み出したり、あるいは IC カードチップ 150 に書  
 き込んだりすることを意味する。

【0072】IC カードチップ 150 の環境設定は、I  
 C カードチップ 150 に IC カードコマンドを N 個 (N  
 は正の整数) 発行することによっておこなう。例えば、  
 セッション鍵が 3 個必要ならば、IC カードコマンドを  
 3 回発行し、セッション鍵が 2 個必要ならば、IC カ  
 ードコマンドを 2 回発行する。N 個の IC カードコマ  
 ンドは、互いに相違するものであってもよいし、同一の  
 ものであってもよい。N の値は固定されたものではなく、  
 状況によってさまざまな値となる。以下、環境設定で発  
 行する IC カードコマンドを、設定コマンドと呼ぶ。ま  
 た、この環境設定に基づいてセキュリティ処理を実行す  
 る IC カードコマンドを、以下、セキュリティコマンド  
 と呼ぶ。セキュリティコマンドの例としては、デジタル  
 署名の計算、デジタル署名の検証、メッセージの暗号  
 化、暗号化メッセージの復号、パスワードによる認証な  
 どをおこなうコマンドがある。

【0073】CPU 121 は、IC カードチップ 150  
 の環境設定の内容を自由に変更することができる。CPU  
 121 は、セキュリティ処理の内容や結果に応じてこ  
 れを変更してもよいし、ホスト機器からのメモリカード  
 コマンドの受信を契機としてこれを変更してもよい。ま  
 た、CPU 121 は、環境設定の内容を示した情報をフラ  
 ッシュメモリチップ 130 にライトし、必要なときに  
 フラッシュメモリチップ 130 からその情報をリードし  
 て使用することもできる。この情報は、図 21 において  
 IC カード環境設定情報 2112 として示されている。  
 これにより、MMC 110 が非活性化されてもその情報  
 を保持することができ、MMC 110 が活性化されるた  
 びにあらためて設定する手間を省くことができる。

【0074】第 1 次 IC カード初期化処理および第 2 次  
 IC カード初期化処理は、IC カード制御パラメータ  
 A、B、C に設定された値に基づいておこなわれる。ま  
 た、CPU 121 は、ステップ 712 で実行するセキュ  
 リティ処理において、IC カード制御パラメータ D に設  
 定された値に基づいて IC カードチップ 150 の活性化  
 や非活性化を制御する。

【0075】図 8 は、IC カード制御パラメータの種類  
 と設定値、それに対応した処理の内容を表している。ま  
 ず、パラメータ A は、MMC 110 に電源が供給され  
 たときに実行される第 1 次 IC カード初期化処理に関  
 するパラメータである。A=0 のときは、CPU 121 は  
 IC カードチップ 150 にアクセスしない。A=1 のとき  
 は、CPU 121 は IC カードチップ 150 をコールド  
 リセットする。A=2 のときは、CPU 121 は IC カ  
 ードチップ 150 をコールドリセットした後で IC カ  
 ードチップ 150 の環境設定をおこなう。A=3 のとき  
 は、CPU 121 は IC カードチップ 150 をコールド  
 リセットした後で IC カードチップ 150 の環境設定を  
 おこない、最後に IC カードチップ 150 を非活性化す  
 る。A=0 または A=3 のときは、第 1 次 IC カード初  
 期化処理のあと IC カードチップ 150 が非活性状態と  
 なる。A=1 または A=2 のときは、第 1 次 IC カード  
 初期化処理のあと IC カードチップ 150 は活性状態と  
 なる。

【0076】次に、パラメータ B と C は、MMC 110  
 が MMC 初期化コマンドを処理したときに実行される第  
 2 次 IC カード初期化処理に関するパラメータである。  
 B=0 のときは、CPU 121 は IC カードチップ 150  
 にアクセスしない。B=1 かつ C=1 のときは、CPU  
 121 は IC カードチップ 150 をリセット (コールド  
 リセットまたはウォームリセット) する。B=1 かつ  
 C=2 のときは、CPU 121 は IC カードチップ 150  
 をリセットした後で IC カードチップ 150 の環境設  
 定をおこなう。B=1 かつ C=3 のときは、CPU 12  
 1 は IC カードチップ 150 をリセットした後で IC カ  
 ードチップ 150 の環境設定をおこない、最後に IC カ

ードチップ150を非活性化する。B=2かつC=2のときは、CPU121はICカードチップ150の環境設定をおこなう。B=2かつC=3のときは、CPU121はICカードチップ150の環境設定をおこなった後にICカードチップ150を非活性化する。B=3のときは、ICカードチップ150が活性状態ならば、CPU121はICカードチップ150を非活性化する。

【0077】最後に、パラメータDは、ホスト機器220から要求されたセキュリティ処理を実行したあとに、ICカードチップ150を非活性化するか否かを示すパラメータである。D=0のときは、セキュリティ処理の実行後に、CPU121はICカードチップ150を非活性化せず、活性状態に保つ。D=1のときは、セキュリティ処理の実行後に、CPU121はICカードチップ150を非活性化する。

【0078】CPU121は、ICカード制御パラメータA、B、C、Dの設定値を変更することができる。CPU121は、セキュリティ処理の内容や結果に応じてこれらの設定値を変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機としてこれらの設定値を変更してもよい。また、CPU121は、これらの設定値をフラッシュメモリチップ130にライトし、必要なときにフラッシュメモリチップ130からこれらの設定値をリードして使用することもできる。これらの設定値は、図21においてICカード制御パラメータ211として示されている。これにより、MMC110が非活性化されてもこれらの設定値を保持することができ、MMC110が活性化されるたびにあらためて設定する手間を省くことができる。

【0079】図9は、第1次ICカード初期化処理の手順を示すフローチャートである。初期化処理を開始する(901)と、まず、ICカード制御パラメータAが0かチェックする(902)。A=0ならばそのまま初期化処理は終了する(908)。A=0でないならばICカードチップ150をコールドリセットする(903)。次に、ICカード制御パラメータAが1かチェックする(904)。A=1ならば初期化処理は終了する(908)。A=1でないならばICカードチップ150の環境設定をおこなう(905)。次に、ICカード制御パラメータAが2かチェックする(906)。A=2ならば初期化処理は終了する(908)。A=2でないならばICカードチップ150を非活性化する(907)。そして、初期化処理は終了する(908)。

【0080】図10は、第2次ICカード初期化処理の手順を示すフローチャートである。初期化処理を開始する(1001)と、まず、ICカード制御パラメータBが0かチェックする(1002)。B=0ならばそのまま初期化処理は終了する(1013)。B=0でないならばB=1かチェックする(1003)。B=1ならばICカード制御パラメータAが0または3かチェックす

る(1004)。Aが0または3ならば、ICカードチップ150をコールドリセットし(1005)、ステップ1007に移る。Aが1または2ならば、ICカードチップ150をウォームリセットし(1006)、ステップ1007に移る。ステップ1007では、ICカード制御パラメータCが1かチェックする。C=1ならば初期化処理は終了する(1013)。C=1でないならばステップ1009に移る。ステップ1003においてB=1でないならば、Bが2かチェックする(1008)。B=2ならばステップ1009に移る。B=2でないならば、ICカード制御パラメータAが0または3かチェックする(1011)。Aが0または3ならば初期化処理を終了する(1013)。Aが1または2ならば、ステップ1012に移る。ステップ1009ではICカードチップ150の環境設定をおこなう。そして、ICカード制御パラメータCが2かチェックする(1010)。C=2ならば初期化処理を終了する(1013)。C=2でないならばステップ1012に移る。ステップ1012ではICカードチップ150を非活性化する。そして、初期化処理を終了する(1013)。

【0081】図11は、ICカードチップ150が非活性状態であるときに第1次ICカード初期化処理あるいは第2次ICカード初期化処理を実行した場合において、ICカードチップ150の外部端子の信号波形を簡単に表した図である。図12は、ICカードチップ150が活性状態であるときに第2次ICカード初期化処理を実行した場合において、ICカードチップ150の外部端子の信号波形を簡単に表した図である。図11と図12において、時間の方向は左から右にとっており、上の行から下の行に向かってVCC2端子151、RST端子152、CLK2端子153、I/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準(Lレベル)を表す。

【0082】図11において1102は、図3に示したコールドリセットの信号波形を表す。図12において1202は、図4に示したウォームリセットの信号波形を表す。図11と図12において、第1設定コマンド処理1104aと1204a、第2設定コマンド処理1104bと1204b、第N設定コマンド処理1104cと1204cは、それぞれ図5に示したICカードコマンド処理の信号波形を表す。ICカードチップ150の環境設定の信号波形1104と1204は、N個の設定コマンド処理の信号波形が連なって構成される。

【0083】図11と図12において、1106と1206は、それぞれ図6に示した非活性化の信号波形を表す。図11と図12において、縦方向の破線1101、1103、1105、1107、1201、1203、1205、及び1207は、それぞれ特定の時刻を表す。1101はコールドリセット前の時刻、1201はウォームリセット前の時刻、1103はコールドリセッ

ト後から環境設定前の間にある時刻、1203はウォームリセット後から環境設定前の間にある時刻、1105と1205は環境設定後から非活性化前の間にある時刻、1107と1207は非活性化後の時刻である。

【0084】図11を参照して、第1次ICカード初期化処理実行時の信号波形を示す。ICカード制御パラメータAが0のときは、信号波形に変化はない。A=1のときは、時刻1101から時刻1103までの範囲の信号波形となる。A=2のときは、時刻1101から時刻1105までの範囲の信号波形となる。A=3のときは、時刻1101から時刻1107までの範囲の信号波形となる。

【0085】図11を参照して、ICカード制御パラメータAが0または3のときの、第2次ICカード初期化処理実行時の信号波形を示す。ICカード制御パラメータBが0のときは、信号波形に変化はない。B=1かつICカード制御パラメータC=1のときは、時刻1101から時刻1103までの範囲の信号波形となる。B=1かつC=2のときは、時刻1101から時刻1105までの範囲の信号波形となる。B=1かつC=3のときは、時刻1101から時刻1107までの範囲の信号波形となる。

【0086】図12を参照して、ICカード制御パラメータAが1または2のときの、第2次ICカード初期化処理実行時の信号波形を示す。ICカード制御パラメータBが0のときは、信号波形に変化はない。B=1かつICカード制御パラメータC=1のときは、時刻1201から時刻1203までの範囲の信号波形となる。B=1かつC=2のときは、時刻1201から時刻1205までの範囲の信号波形となる。B=1かつC=3のときは、時刻1201から時刻1207までの範囲の信号波形となる。B=2かつC=2のときは、時刻1203から時刻1205までの範囲の信号波形となる。B=2かつC=3のときは、時刻1203から時刻1207までの範囲の信号波形となる。B=3のときは、時刻1205から時刻1207までの範囲の信号波形となる。

【0087】図13は、図7のステップ712において、CPU121が、ホスト機器220が要求したセキュリティ処理をICカードチップ150によって実行するときの手順を示すフローチャートである。セキュリティ処理を開始する(1301)と、まずICカードチップ150が非活性状態かをチェックする(1302)。非活性状態ならば、ICカードチップ150をコールドリセットし(1303)、ステップ1306に移る。活性状態ならば、ステップ1304に移る。ステップ1304では、ICカードチップ150にICカードコマンドを発行する前にICカードチップ150を再リセットする必要があるかをチェックする。必要があるならば、ICカードチップ150をウォームリセットし(1305)、ステップ1306に移る。必要がないならば、ス

テップ1306に移る。ステップ1306では、ICカードチップ150の環境設定をおこなう必要があるかをチェックする。必要があるならば、ICカードチップ150の環境設定をおこない(1307)、ステップ1308に移る。必要がないならば、ステップ1308に移る。ステップ1308では、ICカードチップ150のCLK2端子に供給するクロック信号の周波数F2を設定する。そして、CPU121はICカードチップ150にセキュリティコマンドを発行し、ICカードチップ150はそれを処理する(1309)。セキュリティコマンドの処理時間は、クロック周波数F2に依存する。

【0088】次に、ICカードチップ150が出力するICカードレスポンスにより、その処理が成功したかどうかを判定する(1310)。成功ならば、ステップ1311に移る。失敗ならば、ステップ1312に移る。ステップ1311では、ICカードチップ150に発行すべきセキュリティコマンドが全て完了したかをチェックする。発行すべきセキュリティコマンドがまだあるならば、ステップ1304に移る。発行すべきセキュリティコマンドが全て完了したならば、ステップ1314に移る。ステップ1312では、失敗したセキュリティコマンドをリトライすることが可能かを判定する。リトライできるなら、リトライ設定をおこない(1313)、ステップ1304に移る。リトライ設定とは、リトライすべきセキュリティコマンドやその関連データをCPU121が再度準備することである。リトライできないならステップ1314に移る。これは、ホスト機器220が要求したセキュリティ処理が失敗したことを意味する。ステップ1314では、ICカード制御パラメータDをチェックする。D=1ならば、ICカードチップ150を非活性化して(1315)、セキュリティ処理を終了する(1316)。D=1でないならば、ICカードチップ150を活性状態に保ったままセキュリティ処理を終了する(1316)。

【0089】図13のフローチャートにおいては、クロック周波数F2を、ステップ1309で発行するセキュリティコマンドの種類によって変えることができるように、ステップ1308をステップ1309の直前に位置させたが、ステップ1308はそれ以外の位置にあってもよい。

【0090】従来のICカードへの攻撃法を有効にしている要因のひとつとして、ICカードの駆動クロックが外部の接続装置から直接供給されることがあげられる。駆動クロックが接続装置の制御下にあるため、タイミング解析や電力差分析においては、電気信号の測定においてICカード内部処理のタイミングの獲得が容易になる。一方、故障利用解析においては、異常な駆動クロックの供給による演算エラーの発生が容易になる。これに対し、本発明によれば、MMC110内部でICカードチップ150によりセキュリティ処理を実行するとき、



ホスト機器 220 は IC カードチップ 150 の駆動クロックを直接供給できない。CPU 121 は、IC カードチップ 150 へ供給するクロックの周波数 F2 を自由に設定することができる。これにより、ホスト機器 220 の要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。ホスト機器 220 が高速なセキュリティ処理を要求するならば周波数 F2 を高く設定し、低い消費電力を要求するならば周波数 F2 を低く設定したり、クロックを適度に停止させればよい。

【0091】また、CPU 121 は、周波数 F2 だけでなくクロックの供給開始タイミング、供給停止タイミングを自由に設定できる。これらをランダムに変化させることにより、IC カードチップ 150 に対するタイミング解析、電力差分析、故障利用解析と呼ばれる攻撃法を困難にすることができる。タイミング解析は、攻撃者が暗号処理 1 回の処理時間を正確に計測可能であることを仮定しているため、その対策としては、攻撃者が処理時間計測を正確に行えないようにすることが有効である。本発明によりタイミング解析が困難になる理由は、IC カードチップ 150 が IC カードコマンドを処理している時間の長さをホスト機器 220 が正確に計測できないためである。電力差分析の対策としては、処理の実行タイミングや順序に関する情報を外部から検出不能にすることが有効である。本発明により電力差分析が困難になる理由は、IC カードコマンドが発行された時刻、発行された IC カードコマンドの内容、発行された IC カードコマンドの順序（IC カードコマンドを複数組み合わせでセキュリティ処理を実行する場合）の検出がホスト機器 220 にとって困難になるためである。故障利用解析の対策としては、IC カードにクロックや電圧や温度等の動作環境検知回路を搭載し、異常を検出したならば処理を停止あるいは使用不能にするという方法が有効である。本発明により故障利用解析が困難になる理由は、CLK 2 制御回路 127 が IC カードチップ 150 に異常な駆動クロックを供給しないことが、ホスト機器 220 が IC カードチップ 150 に演算エラーを発生させるのを防止するからである。

【0092】CPU 121 は、IC カードチップ 150 に供給するクロックの周波数 F2、供給開始タイミング、及び供給停止タイミングの設定値を、セキュリティ処理の内容や結果に応じて変更してもよいし、ホスト機器からのメモリカードコマンドの受信を契機として変更してもよい。また、CPU 121 は、これらの設定値をフラッシュメモリチップ 130 にライトし、必要なときにフラッシュメモリチップ 130 からこれらの設定値をリードして使用することもできる。これらの設定値は、図 21 において CLK 2 設定情報 2113 として示されている。これにより、MMC 110 が非活性化されてもこれらの設定値を保持することができ、MMC 110 が活性化されるたびにあらためて設定する手間を省くこと

ができる。

【0093】図 14 は、ホスト機器 220 がセキュリティ処理要求ライトコマンドを MMC 110 に発行してから、IC カードチップ 150 でセキュリティ処理が実行されるまでの過程（図 7 のステップ 710～712）において、MMC 110 および IC カードチップ 150 の外部端子の信号波形、CPU 121 によるフラッシュメモリチップ 130 へのアクセスを簡単に表した図である。図 14 において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ 130 へのアクセス内容である。上から二行目の行から下の行に向かって、VCC1 端子 144、CMD 端子 142、CLK1 端子 145、DAT 端子 147、VCC2 端子 151、RST 端子 152、CLK2 端子 153、及び I/O 端子 157 で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（L レベル）を表す。

【0094】図 14 を参照して、ホスト機器 220 がセキュリティ処理要求ライトコマンドを MMC 110 に発行してから、IC カードチップ 150 でセキュリティ処理が実行されるまでの過程を説明する。まず、ホスト機器 220 は CMD 端子 142 にセキュリティ処理要求ライトコマンドを送信する（1401）。次に、ホスト機器 220 は CMD 端子 142 からセキュリティ処理要求ライトコマンドのレスポンスを受信する（1402）。このレスポンスは、MMC 110 がコマンドを受信したことをホスト機器 220 に伝えるものであり、セキュリティ処理の実行結果ではない。次に、ホスト機器 220 は DAT 端子 147 にセキュリティ処理要求を送信する（1403）。セキュリティ処理要求とは、セキュリティ処理の内容や処理すべきデータを含むホストデータである。次に、MMC 110 は DAT 端子 147 を L レベルにセットする（1404）。MMC 110 は、これによりビジー状態であることをホスト機器 220 に示す。次に、CPU 121 は、ホスト機器 220 から受信したセキュリティ処理要求をフラッシュメモリチップ 130 にライトするコマンドを発行する（1405）。セキュリティ処理要求をフラッシュメモリチップ 130 にライトすることにより、CPU 121 がセキュリティ処理要求を IC カードコマンド形式で記述する処理（図 7 のステップ 711）において、CPU 121 内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求のデータサイズが大きいために有効である。

【0095】なお、フラッシュメモリチップ 130 にライトされたセキュリティ処理要求は、図 21 においてセキュリティ処理バッファ領域 2114 に格納される。また、ライトコマンド発行 1405 は必須な操作ではない。ライト処理期間 1406 は、フラッシュメモリチップ 130 がセキュリティ処理要求のライト処理を実行している期間を表す。セキュリティ処理 1407 は IC カードチップ 150 によるセキュリティ処理の信号波形を



表す。この信号波形は図 13 のフローチャートの遷移過程に依存する。セキュリティ処理 1407 は、ライト処理期間 1406 とオーバーラップさせることができる。一般にフラッシュメモリチップ 130 のライト処理期間 1406 はミリ秒のオーダーであるため、セキュリティ処理 1407 とオーバーラップさせることは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。リード／ライト 1408 は、セキュリティ処理 1407 の実行中に、フラッシュメモリチップ 130 からセキュリティ処理要求をリードしたり、IC カードチップ 150 が出力した計算結果をフラッシュメモリチップ 130 にライトするアクセスを示している。このアクセスにより、CPU 121 内部のワークメモリの消費量を節約できる。これは、セキュリティ処理要求やセキュリティ処理結果のデータサイズが大きいときに有効である。リード／ライト 1408 は必須ではない。セキュリティ処理 1407 が完了したら、MMC 110 は DAT 端子 147 を H レベルにセットする (1409)。MMC 110 は、これによりセキュリティ処理が完了したことをホスト機器 220 に示す。

【0096】図 15 は、図 14 におけるセキュリティ処理 1407 の信号波形の一例を表した図である。図 15 において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ 130 へのアクセス内容である。上から二行目の行から下の行に向かって、VCC2 端子 151、RST 端子 152、CLK2 端子 153、及び I/O 端子 157 で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準 (L レベル) を表す。1501 は図 3 に示したコールドリセットの信号波形を表し、1504 は図 4 に示したウォームリセットの信号波形を表し、1502 および 1505 は図 11 (あるいは図 12) に示した環境設定の信号波形を表し、1503 および 1506 および 1507 は図 5 に示した IC カードコマンド処理の信号波形を表し、1508 は図 6 に示した非活性化の信号波形を表す。IC カードチップ 150 の外部端子において図 15 に示した信号波形が観測されるのは、図 13 のフローチャートが 1301、1302、1303、1306、1307、1308、1309、1310、1311、1304、1305、1306、1307、1308、1309、1310、1311、1304、1306、1308、1309、1310、1311、1314、1315、1316 の順で遷移するときである。

【0097】図 15 を参照して、図 14 のセキュリティ処理 1407 の実行中における CPU 121 によるフラッシュメモリチップ 130 へのアクセス (リード／ライト 1408) を説明する。このアクセスには、図 21 におけるセキュリティ処理バッファ領域 2114 を使用する。リード 1509、1511、及び 1512 は、それぞれ、セキュリティコマンド処理 1503、1506、

及び 1507 において IC カードチップ 150 に送信する IC カードコマンドを構築するために必要なデータを、フラッシュメモリチップ 130 からリードするアクセスである。ライト 1510 は、セキュリティコマンド処理 1503 において IC カードチップ 150 が出力した計算結果を、フラッシュメモリチップ 130 にライトするアクセスである。ライト 1513 は、セキュリティコマンド処理 1506 及び 1507 において IC カードチップ 150 が出力した計算結果を、フラッシュメモリチップ 130 にまとめてライトするアクセスである。リード 1509、1511、1512 は、それぞれ、セキュリティコマンド処理 1503、1506、1507 以前の IC カードチップ 150 へのアクセスとオーバーラップさせることができる。ライト 1510、1513 は、それぞれ、セキュリティコマンド処理 1503、1507 以後の IC カードチップ 150 へのアクセスとオーバーラップさせることができる。これらのオーバーラップは、セキュリティ処理の全体的な処理時間の短縮にとって有効である。さらに、フラッシュメモリチップ 130 のライト単位が大きい場合は、ライト 1513 のように複数の計算結果をまとめてライトすることができる。これは、フラッシュメモリチップ 130 へのライト回数を削減し、フラッシュメモリチップ 130 の劣化を遅らせる効果がある。なお、ライト 1510、1513 でフラッシュメモリチップ 130 にライトする内容は、IC カードチップ 150 が出力した計算結果そのものに限定されず、図 7 のステップ 715 でホスト機器 220 に返すセキュリティ処理結果またはその一部であってもよい。この場合、図 7 のステップ 714 またはその一部は、ステップ 712 の中で実行されることになる。

【0098】図 16 は、ホスト機器 220 がセキュリティ処理結果リードコマンドを MMC 110 に発行してから、MMC 110 がセキュリティ処理結果を出力するまでの過程 (図 7 のステップ 713 ~ 715) において、MMC 110 の外部端子の信号波形、CPU 121 によるフラッシュメモリチップ 130 へのアクセスを簡単に表した図である。図 16 において、時間の方向は左から右にとる。一番上の行はフラッシュメモリチップ 130 へのアクセス内容である。上から二行目の行から下の行に向かって、VCC1 端子 144、CMD 端子 142、CLK1 端子 145、及び DAT 端子 147 で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準 (L レベル) を表す。

【0099】図 16 を参照して、ホスト機器 220 がセキュリティ処理結果リードコマンドを MMC 110 に発行してから、MMC 110 がセキュリティ処理結果を出力するまでの過程を説明する。まず、ホスト機器 220 は CMD 端子 142 にセキュリティ処理結果リードコマンドを送信する (1601)。次に、ホスト機器 220 は CMD 端子 142 からセキュリティ処理結果リードコ

マンドのレスポンスを受信する(1602)。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものであり、セキュリティ処理結果ではない。次に、MMC110はDAT端子147をLレベルにセットする(1603)。MMC110は、これによりビジー状態であることをホスト機器220に示す。次に、CPU121は、フラッシュメモリチップ130のセキュリティ処理バッファ領域(図21の2114)から、ICカードチップ150が出力した計算結果をリードする(1604)。CPU121は、これをもとにセキュリティ処理結果を構築し、MMC110がDAT端子147にセキュリティ処理結果を出力する(1605)。なお、図7のステップ714またはその一部が、ステップ712の中で実行されている場合、ステップ1604ではフラッシュメモリチップ130のセキュリティ処理バッファ領域(図21の2114)からセキュリティ処理結果またはその一部をリードする。なお、フラッシュメモリチップ130のセキュリティ処理バッファ領域(図21の2114)を利用しないでセキュリティ処理結果を構築する場合、ステップ1604は必要ない。

【0100】MMC110の製造者や管理者は、セキュリティシステムのユーザにMMC110を提供する前やそのユーザが所有するMMC110に問題が発生した時に、MMC110に内蔵されたICカードチップ150に様々な初期データを書きこんだり、ICカードチップ150のテストをおこなったりする必要がある。MMC110の製造者や管理者によるこれらの操作の利便性を高めるために、MMC110は、ICカードチップ150の外部端子をMMC外部端子140に割りつけるインタフェース機能を持つ。これにより、図3～図6で示したようなICカードチップ150へのアクセス信号を、MMC外部端子140から直接送受信できる。このようなMMC110の動作モードを、MMC仕様に準拠した動作モードと区別して、以下、インタフェース直通モードと呼ぶ。

【0101】インタフェース直通モードについて詳細に説明する。図17は、ICカードチップ150の外部端子をMMC外部端子140に割りつけるときの対応関係の一例を表した図である。この例では、RST端子152をCS端子141に割り付け、GND2端子155をGND1端子143、146に割り付け、VCC2端子151をVCC1端子144に割り付け、CLK2端子153をCLK1端子145に割り付け、I/O端子157をDAT端子147に割り付ける。このとき、CS端子141とCLK1端子145は入力端子、DAT端子147は入出力端子として機能する。

【0102】MMC110は、特定のメモリカードコマンドを受信すると、動作モードをインタフェース直通モードへ移したり、インタフェース直通モードからMMC

仕様に準拠した動作モードに戻ることができる。以下、動作モードをインタフェース直通モードへ移すメモリカードコマンドを直通化コマンド、動作モードをインタフェース直通モードから通常の状態に戻すメモリカードコマンドを復帰コマンドと呼ぶ。図1を参照して、MMC1/F制御回路123は、VCC2制御回路126、CLK2制御回路127、ICカードI/F制御回路128と接続されており、MMC110がホスト機器220から直通化コマンドを受信すると、CPU121の指示により図17で示した端子割り付けをおこなう。MMC110がホスト機器220から復帰コマンドを受信すると、CPU121の指示により図17で示した端子割り付けを解除し、MMC110はMMC仕様に準拠した動作モードに戻る。

【0103】インタフェース直通モードでは、ホスト機器220がICカードチップ150に直接アクセスできるため、セキュリティの観点からインタフェース直通モードを利用できるのは限られた者だけに必要がある。そこで、直通化コマンドの発行には、一般のユーザに知られないパスワードの送信を必要とする。正しいパスワードが入力されないとインタフェース直通モードは利用できない。

【0104】図18は、ホスト機器220が、MMC110の動作モードをMMC仕様に準拠した動作モードからインタフェース直通モードに移し、ICカードチップ150に直接アクセスし、その後、MMC110の動作モードを再びMultiMediaCard仕様に準拠した動作モードに戻すまでの処理手順を示すフローチャートである。ホスト機器220は処理を開始し(1801)、まずMMC110に直通化コマンドを発行する(1802)。MMC110は、直通化コマンドで送信されたパスワードが正しいかチェックする(1803)。正しければステップ1804に移り、間違っていれば処理は終了する(1810)。ステップ1804では、CPU121は、ICカードチップ150をコールドリセットする。そして、図17で示した端子割り付けをおこないインタフェースを直通化する(1805)。この時点から、ホスト機器220はICカードチップ150に直接アクセスする(1806)。ホスト機器220がICカードチップ150への直接アクセスを終了し、MMC110の動作モードを再びMMC仕様に準拠した動作モードに戻すときは、MMC110に復帰コマンドを発行する(1807)。すると、CPU121は図17で示した端子割り付けを解除し、MMC110はMMC仕様に準拠した動作モードに戻る(1808)。そして、CPU121は、ICカードチップ150を非活性化する(1809)。以上で、処理は終了する(1810)。

【0105】図19は、図18のステップ1801～1806の過程において、MMC110およびICカード

チップ150の外部端子の信号波形を簡単に表した図である。図19において、時間の方向は左から右にとる。上の行から下の行に向かって、VCC1端子144、CMD端子142、CLK1端子145、DAT端子147、VCC2端子151、RST端子152、CLK2端子153、及びI/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Lレベル）を表す。1905は、図3のコールドリセットの信号波形を示す。モード移行時刻1906は、動作モードがインタフェース直通モードに移る時刻を表す。

【0106】図19を参照して、ホスト機器220がMMC110の動作モードをMMC仕様に準拠した動作モードからインタフェース直通モードに移しICカードチップ150に直接アクセスする過程を説明する。なお、MMC110のVCC1端子144には3V（VCC2端子151の標準電圧）が供給されている。ホスト機器220がCMD端子142に直通化コマンドを入力すると（1901）、CMD端子142から直通化コマンドのレスポンスが出力される（1902）。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものである。次に、ホスト機器220はDAT端子147にパスワードを入力する（1903）。パスワード入力後、MMC110はDAT端子147にLレベルを出力し（1904）、ビジー状態であることをホスト機器220に示す。ビジー状態の間に、CPU121は、ICカードチップ150をコールドリセットする（1905）。そして、モード移行時刻1906において、動作モードをインタフェース直通モードに移す。このときに、DAT端子147はLレベルからハイインピーダンス状態になる。これにより、ホスト機器220はビジー状態の解除を知ることができる。この時点から、ホスト機器220はICカードチップ150に直接アクセスする。例えば、CLK1端子145にクロックを供給すると（1907）、CLK2端子153にそのクロックが供給される（1908）。また、DAT端子147にICカードコマンドを送信すると（1909）、I/O端子157にそのICカードコマンドが送信される（1910）。

【0107】図20は、図18のステップ1807～1810の過程において、MMC110およびICカードチップ150の外部端子の信号波形を簡単に表した図である。図20において、時間の方向は左から右にとる。上の行から下の行に向かって、VCC1端子144、CMD端子142、CLK1端子145、DAT端子147、VCC2端子151、RST端子152、CLK2端子153、及びI/O端子157で観測される信号を表す。また、横方向の破線はそれぞれの信号の基準（Lレベル）を表す。モード復帰時刻2003は、動作モードがインタフェース直通モードからMMC仕様に準拠した動作モードに戻る時刻を表す。2004は、図6の非

活性化の信号波形を示す。

【0108】図20を参照して、ホスト機器220がMMC110の動作モードをインタフェース直通モードからMMC仕様に準拠した動作モードに戻す過程を説明する。なお、MMC110のVCC1端子144には3V（VCC2端子151の標準電圧）が供給されている。ホスト機器220がCMD端子142に復帰コマンドを入力すると（2001）、CMD端子142から復帰コマンドのレスポンスが出力される（2002）。このレスポンスは、MMC110がコマンドを受信したことをホスト機器220に伝えるものである。そして、モード復帰時刻2003において、MMC110はDAT端子147にLレベルを出力してビジー状態であることをホスト機器220に示し、それと同時に動作モードをMMC仕様に準拠した動作モードに戻す。ビジー状態の間に、CPU121は、ICカードチップ150を非活性化（2004）。そして、MMC110は、DAT端子147をハイインピーダンス状態にし（2005）、復帰コマンドの処理が完了したことをホスト機器220に示す。これ以後、ホスト機器220はICカードチップ150に直接アクセスできない。ホスト機器220が、CLK1端子145にクロックを供給しながらCMD端子142に何らかのメモリカードコマンドを送信した場合、ICカードチップ150にそのクロック信号（2006）は伝わらない。2001及び2002においてホスト機器220がCLK1端子145に供給するクロック信号は、ICカードチップ150のCLK2端子153にも伝わるが、DAT端子147がハイインピーダンス状態であるため、ICカードチップ150がICカードコマンドを誤って認識することはない。

【0109】図21において、セキュリティ処理ステータス領域2116には、ICカードチップ150によるセキュリティ処理の進捗状況を示す情報を格納する。CPU121は、この情報をセキュリティ処理の実行中に更新することができる。例えば、セキュリティ処理の途中でMMC110への電源供給が停止した場合、電源供給再開時にCPU121がこの情報をリードして参照すれば、セキュリティ処理を中断した段階から再開することができる。

【0110】本発明におけるMMC110は、コントローラチップ120、フラッシュメモリチップ130及びICカードチップ150の三つのうち二つ以上のチップで同時に処理を行うことで、処理の高速化及び処理時間の短縮を図ることができる。以下、本発明を適用したMMC110で行える並列処理の動作について説明する。

図27は、並列に処理できるデータリード処理の手順を示したフローチャートである。ホスト機器220とMMC110は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態2701、待機状態2719となっている。ホスト機器220がMMC

110のCMD端子142に第一コマンドを送信すると(2702)、MMC110は、第一コマンドを受信し(2709)、第一レスポンスを返す(2710)。ここで、レスポンスとは、コマンドを受け取ったMMC110がホスト機器220に返すデータのことである。単にコマンドを受信したら返すデータであるので、レスポンスを返すことがコマンドの実行が終了したことを意味しない。

【0111】MMC110のコントローラチップ120は、第一コマンドを解釈し、フラッシュメモリチップ130又はICカードチップ150に制御命令を発し第一処理に入る(2715)。ホスト機器220は、第一レスポンスを受け取ると第二コマンドを送信する(2704)。MMC110のコントローラチップ120は、第一処理を実行しながら、ホスト機器220より第二コマンドを受信し、(2705)、第二レスポンスを返す(2712)。コントローラチップ120は、第二コマンドを解釈し、第二処理を実行する(2713)。

【0112】第二コマンドは、あらかじめ第一コマンドと同時に処理できるコマンドをホスト機器220で判定し設定する。また、同時に処理できるコマンドの判定は、コントローラチップ120でおこなってもよい。以下、同時に実行できるコマンドのことを並列実行可能なコマンドと呼ぶ。並列実行可能なコマンドとしては、例えば、フラッシュメモリチップ130にアクセスするコマンドとICカードチップ150にアクセスするコマンド等の異なったチップにアクセスするコマンドである。例えば、フラッシュメモリチップ130から音楽データを読み出すコマンドが第一コマンドに相当し、暗号化されたデータを復号化する処理を実行するコマンドが第二コマンドに相当する。

【0113】第一処理が終了すると、コントローラチップ120は、ホスト機器220に第一データを送信する(2716)。その後、第二データを送信する(2714)。第一データ及び第二データの区別は、MMC110のコントローラチップ120とホスト機器220のホストインターフェース223でデータに識別情報を付加して管理判断する。以下、識別情報を付加したデータをデータと呼ぶ。

【0114】また、第一処理の転送が終了して、第二処理をしている間にホスト機器220が並列実行可能なコマンドを第三コマンドとして発行した場合は、コントローラチップ120は、第二処理の実行とあわせて第三コマンドのコマンドを解釈し、第三処理を実行する(2717)。もし第一コマンドが大容量のデータ(ストリームデータ等)を要求するコマンドであるならば、第三処理を実行し(2717)、第二データの送信の終了を待ち、第三データを送信する(2718)。その後ホスト機器220からコマンドがなければ、MMC110は待機状態になる(2719)。ホスト機器220はMMC

110から必要なデータを受け取ると、待機状態になる(2701)。

【0115】図28は、リードコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸に示した図である。ホスト機器220は、MMC110のCMD端子142に第一コマンドを送信する(2702)。コントローラチップ120は、第一コマンドを解釈し、フラッシュメモリチップ130に制御命令を出す。第一処理中(2715)に、ホスト機器220は、並列実行可能なコマンドを第二コマンドとしてMMC110のCMD端子142に送信する(2704)。コントローラチップ120は、第二コマンドを解釈し、ICカードチップ150に制御命令を出し、第二処理を実行する(2713)。MMC110は、第一データ2803、第二データ2804のように順にデータを転送する。第二処理(2713)中にホスト機器220が第三コマンドとしてフラッシュメモリチップ130にアクセスするコマンドを発行した場合(2801)、コントローラチップ120はフラッシュメモリチップに制御命令を出す。MMC110は、第二データ2804の転送終了を待って、第三データ2805を転送する。また第三データ2805は、第一コマンドが大容量データ(ストリームデータ等)を送るコマンドでもよい。その場合は、第三コマンドの発行(2801)と第三レスポンス(2802)の信号はなくてもよい。以上の処理内容は、コントローラチップ120が制御命令を出す対象としてフラッシュメモリチップ130がICカードチップ150で、ICカードチップ150がフラッシュメモリチップ130のように逆の場合でもよい。

【0116】図29は、並列に処理できるデータライト処理の流れを示した図である。ホスト機器220とMMC110は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態2901及び待機状態2910となっている。ホスト機器220がMMC110のCMD端子142に第一コマンドを送信する(2902)。MMC110は、第一コマンドを受信し(2911)、第一レスポンスを返し(2912)、同時に第一データを受信し(2913)、データ端子147からデータを転送できないようにする。これを以下ビジー状態と呼ぶ。MMC110はホスト機器220からデータを受け取った後ビジー状態にしなくても良い。第一データを受信するステップ2913は、第一レスポンス(2912)と同時になくても良い。

【0117】ホスト機器220は、第一レスポンスを受信し(2903)、並列実行可能なコマンドを第二コマンドとして、CMD端子142に送信する(2904)。MMC110は、ホスト機器220より第二コマンドを受信し(2914)、第一データを受信(2913)中であれば受信し、第二レスポンスを送信し(2915)、第二処理を開始する(2920)。データビジ

一状態であれば、第二処理で行うアドレス設定まで行い、第二データの転送を待つ。第二処理はアドレス設定のみだけでなく実行可能な処理を続けてもよい。ホスト機器 220 は、第二レスポンスを受信し (2905)、ビジー状態の解除を待って、第二データを送信する (2907)。第一コマンドが大容量データ (ストリームデータ等) を転送する場合、MMC 110 は、第二処理中 (2920) に第三処理を開始し (2921)、第三データの転送 (2908) を待つ。MMC 110 は、ビジー状態が解除されたら、第三データを受信し (2918)、第三処理を続ける。その後ホスト機器 220 からコマンドがなければ、MMC 110 は待機状態になる (2910)。ホスト機器 220 は MMC 110 に必要なデータを転送し終わると、待機状態になる (2901)。

【0118】図 30 は、ライトコマンドを並列処理する時のコマンドとデータの流れ及び処理を時間軸にそって示した図である。ホスト機器 220 がフラッシュメモリチップ 130 にデータをライトする第一コマンドを MMC 110 の CMD 端子 142 に送信し (2902)、第一レスポンスを待ち (2903)、第一データを送信する (3003)。MMC 110 は、第一コマンドを受けると第一レスポンスを送信し (2903)、フラッシュメモリチップ 130 に制御命令を出し (第一処理 2916)、ビジー状態となる。ここでビジー状態にしなくてもよい。ホスト機器 220 は、第一データ 3003 を送信しながら並列実行可能なコマンドとして IC カードチップ 150 にデータを転送する第二コマンドを送信する (2904)。ホスト機器 220 は、第二レスポンスを受信し (2905)、ビジー状態の解除を待って第二データ 3004 を送信する。コントローラチップ 120 は、IC カードチップ 150 に制御命令を出し、第二処理を開始して、第二データ 3004 を待つ。ホスト機器 220 は、ビジー状態が解除されると IC カードチップ 150 に送信する第二データ 3004 を転送する。

【0119】MMC 110 は、第二データを受信すると (2917)、ビジー状態になる。IC カードチップ 150 が処理中 (第二処理中 2920) に、ホスト機器 220 がフラッシュメモリチップ 120 にアクセスする第三コマンドの発行すると (3001)、MMC 110 は、第三レスポンスを送信し (3002)、コントローラチップ 120 はフラッシュメモリチップに制御命令を出し、第三処理を開始する (2921)。ホスト機器 220 は、ビジー状態の解除を待って第三データを送信する (3005)。もしフラッシュメモリチップ 130 にアクセスする第一コマンドが大容量データ (ストリームデータ等) を転送する場合は、IC カードチップ 150 の処理中 (第二処理 2920) のビジー状態の解除を待って、ホスト機器 220 は、フラッシュメモリチップ 130 に第三データ 3005 を送信する。MMC 110 は、

第三データ 3005 を受信し、フラッシュメモリチップ 130 に制御命令を出し第三処理を行う。

【0120】以上の処理内容は、コントローラチップ 120 が制御命令を出す対象としてフラッシュメモリチップ 130 が IC カードチップ 150 で、IC カードチップ 150 がフラッシュメモリチップ 130 のように逆の場合でもよい。

【0121】図 31 は、並列に処理できるデータを転送しないコマンドの処理を示した図である。ホスト機器 220 及び MMC 110 は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態 3101、待機状態 3110 となっている。ホスト機器 220 は MMC 110 の CMD 端子 142 に第一コマンドを送信する (3102)。MMC 110 は、第一コマンドを受信し (3111)、第一レスポンスをホスト機器 220 に送信し (3112)、第一処理を開始する (3116)。ホスト機器 220 は MMC 110 からの第一レスポンスを受信すると (3103)、並列実行可能なコマンドを第二コマンドとして送信する (3104)。MMC 110 は、第二コマンドを受信すると (3113)、ホスト機器 220 に対し第二レスポンスを送信し (3114)、第二処理を実行する (3115)。その後処理が終わると、ホスト機器 220 は待ち状態 3101、MMC 110 は待ち状態 3110 の状態となる。

【0122】図 32 は、並列に処理できるデータを転送しないコマンドの実行する時の処理を時間軸にそって示した図である。ホスト機器 220 は、MMC 110 の CMD 端子 142 にデータ転送を行わないフラッシュメモリチップ 130 にアクセスする第一コマンドを送信する (3102)。MMC 110 は、第一コマンドを受信し (3111)、コントローラチップ 120 は、フラッシュメモリチップ 130 に制御命令を出し、第一処理を開始する (3114)。ホスト機器 220 は、第一レスポンスを受信し (3103)、MMC 110 の CMD 端子 142 にデータ転送を行わない IC カードチップ 150 にアクセスする第二コマンドを送信する (3104)。MMC 110 は、第二コマンドを受信し (3113)、コントローラチップ 120 は、IC カードチップ 150 に制御命令を出し第二処理を行う (3115)。ホスト機器 220 は、コントローラチップ 120 の内部処理のみで実行できるコマンドを第三コマンドとして MMC 110 の CMD 端子 142 に送信する (3201)。MMC 110 は第三コマンドを受信し、第三処理を実行する (3203)。このとき、第一処理及び第二処理は実行中でもよい。

【0123】以上の処理の中で、第一コマンド及び第二コマンドは、フラッシュメモリチップ 130 にアクセスする処理、IC カードチップ 150 にアクセスする処理、及びコントローラチップ 120 の内部処理の三処理のうちのどの二処理でもよい。また、連続コマンドが、

コントローラチップ120の内部処理のみで実行できるコマンドで、同様の処理を行うコマンドは、後で発行したコマンドだけを有効にしても良い。

【0124】図33は、並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを示した図である。ホスト機器220及びMMC110は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態3301、待機状態3310となっている。ホスト機器220がMMC110のCMD端子142に第一コマンドを送信する(3302)。MMC110は第一コマンドを受信し(3311)、第一レスポンスをホスト機器220に送信し(3312)、第一処理を開始する(3316)。ホスト機器220は、第一レスポンスを受信して(3303)、並列実行可能なコマンドを第二コマンドとして送信する(3304)。MMC110は、第二コマンドを受信し(3313)、第二レスポンスを返す(3314)。その間にDAT端子147から、第一データを送信し(3317)、第二処理を開始する(3315)。ホスト機器220は、第一データを受信し(3306)、第二レスポンスを受信する(3305)。ホスト機器220は、並列処理可能なコマンドとして第三コマンドを送信する(3307)。MMC110は、第三コマンドを受信し(3318)、第三レスポンスを返す(3319)。ホスト機器220は、第三レスポンスを受信する(3308)。MMC110は、第三処理3120を実行し、第二データを送信する(3321)。ホスト機器220は、第二データを受信する(3309)。その後実行するコマンドがなければ、ホスト機器220は、待ち状態3301に、MMC110は、待ち状態3310になる。

【0125】図34は、並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。ホスト機器220がMMC110のコマンド端子142にフラッシュメモリチップ120にアクセスする第一コマンドを送信する(3302)。MMC110は第一レスポンスを返し(3303)、コントローラチップ120は、制御命令をフラッシュメモリチップ130に出し第一処理を開始する(3317)。ホスト機器220は、並列実行可能なデータ転送を伴わないICカードチップ150にアクセスする第二コマンドを送信する(3304)。MMC110は第二コマンドを受信して(3313)、第二レスポンスを返し(3305)、コントローラチップ120はICカードチップ150に制御命令を出し、第二処理を開始する(3315)。MMC110は、第一処理が終了すると(3316)、第一データ3403をホスト機器220に送信する。ホスト機器220は、第一データを受信し(3306)、並列処理可能なフラッシュメモリチップ130にアクセスする第三コマンドを送信する(3307)。MMC110は、第三レスポンスを返し(3

308)、コントローラチップ120は第三処理を実行し(3320)、第二データを送信する(3405)。

【0126】以上の処理は、フラッシュメモリチップ130がICカードチップ150で、ICカードチップ150がフラッシュメモリチップ130のように逆でもよい。また、データ転送を伴わないコマンドは、コントローラチップ120の内部処理を行うコマンドでもよい。第一コマンドが大容量データデータ(ストリームデータなど)を転送するコマンドの場合は、第三コマンドは、発行されなくても良い。

【0127】図35は、並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを示した図である。ホスト機器220及びMMC110は、電源投入後コマンド処理が実行できるように初期設定を終了して、各々待機状態3501、待機状態3510となっている。ホスト機器220がMMC110のCMD端子142に第一コマンドを送信する(3502)。MMC110は第一コマンドを受信し(3511)、第一レスポンスをホスト機器220に送信する(3512)。ホスト機器220は、第一レスポンスを受信して(3503)、並列実行可能なコマンドを第二コマンドとして送信し(3504)、第一データを送信する(3505)。MMC110は、第二コマンドを受信し(3513)、第二レスポンスを返す(3514)。その間にDAT端子147から、第一データを受信し(3516)ビジー状態になる。MMC110は、第一データを受信したら(3516)、第一処理を開始し(3517)、第二処理を開始する(3515)。ホスト機器220は、ビジー状態が解除されると第三コマンドを送信(3507)する。MMC110は第三レスポンスを返す(3519)。ホスト機器110は第三レスポンスを受信すると(3508)、第二データを送信する(3509)。MMC110は、第二データを受信し(3520)、ビジー状態になり第三処理(3521)を実行する。処理が終了すると、ホスト機器220は、待ち状態3501となり、MMC110は処理が終了すると待ち状態3510となる。以上の処理で、MMC110がデータ受信後ビジー状態にならなくても良い。

【0128】図36は、並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。ホスト機器220がフラッシュメモリチップ130にアクセスする第一コマンドを転送する(3502)。MMC110は第一レスポンスを返し(3503)、第一データ受信し(3505)、コントローラチップ120はフラッシュメモリチップ130に制御命令を出し、第一処理を開始し(3517)、ビジー状態となる。ホスト機器220は、並列実行可能なデータ転送を伴わないICカードチップ150にアクセスする第二コマンドを送信する(3504)。MMC110は第二コマンドを受信して(351



3)、第二レスポンスを返す(3506)。コントローラチップ120は、ICカードチップ150に制御命令をだし第二処理を開始する(3515)。その後ホスト機器220はビジー状態が解除されるのを待って、フラッシュメモリチップ130にアクセスする第三コマンドを送信する(3507)。MMC110は、第三コマンドを受信し(3518)、第三レスポンスを返し(3508)、第二データ3509を受信する(3520)。コントローラチップ120は、フラッシュメモリチップ130に制御命令を出し、第三処理を開始しビジー状態になる(3521)。

【0129】以上の処理で、フラッシュメモリチップ130がICカードチップ150に、ICカードチップ150がフラッシュメモリチップ130のように逆になっても良い。データ転送を伴わない処理は、コントローラチップ120の内部処理でもよい。また、MMC110がデータ受信後ビジー状態にならなくても良い。第一コマンドが大容量データ(ストリームデータ等)を転送するコマンドである場合、第三コマンドの発行と第三レスポンスは必要としない。

【0130】以上の動作は、図24及び図25で示す、SDカードホスト機器2460とSDカード2410、メモリスティックホスト機器2560とメモリスティック2510のような構成で、コントローラを通してのSDカード内のICカードチップ150とフラッシュメモリチップ2430、メモリスティック内のICカードチップ150とフラッシュメモリチップ2530の同時アクセスの場合においても同様である。

【0131】以上のように、ホストからのコマンドに応じて、フラッシュメモリチップ130、ICカードチップ150及びコントローラチップ120で並列処理が可能であるので処理を高速化及び処理時間を短縮することができる。したがって、一つのMMC110を用いて、音楽データを再生しながら、銀行からお金を引き落とす際の認証処理を行うことができる。

【0132】本発明の実施形態によれば、メモ리카ード外部からICチップの駆動クロックを直接供給しないため、ICチップの処理時間を正確に計測できず、また、処理の実行タイミングや順序の検出が困難になる。さらに、異常な駆動クロックを供給することができず、演算エラーを発生させるのが困難になる。したがって、タイミング解析、電力差分析、故障利用解析攻撃法に対するセキュリティが向上する。

【0133】本発明の実施形態によれば、メモ리카ード外部からICチップの制御方式を自由に設定できる。例えば、高速処理が要求されるならば、ICチップの駆動クロックの周波数を高くした制御方式を設定し、低消費電力が要求されるならば、ICチップの駆動クロックの周波数を低くしたり、ICチップの駆動クロックを適度に停止させる制御方式を設定することができる。したが

って、セキュリティシステムの要求する処理性能に柔軟に対応したセキュリティ処理が実現できる。

【0134】本発明の実施形態によれば、ICチップによるセキュリティ処理に必要なデータや、ICチップを管理するための情報を、フラッシュメモリに保持することができる。したがって、セキュリティ処理の利便性を向上させることができる。

【0135】本発明の実施形態によれば、MMCの製造者や管理者が、MMC内部のICチップに直接アクセスすることができる。したがって、MMC内部のICチップの初期化やメンテナンスを、従来のICカードと同様な方法で実現できる。

【0136】本発明の実施形態によれば、フラッシュメモリチップを備えたMMCに、セキュリティ機能を追加する場合、セキュリティ評価機関の認証を予め受けたICカードチップ追加搭載することによって、セキュリティ評価機関によるMMCの認証が不要となるため、MMCの開発期間又は製造期間が短縮する。

【0137】本発明の実施形態によれば、ホスト機器からのコマンドに応じて、フラッシュメモリチップ、ICカードチップ及びコントローラチップ120で並列処理が可能であるので処理を高速化することができる。

【0138】

【発明の効果】本発明によれば、記憶装置のセキュリティを向上するという効果を奏する。また、記憶装置の処理を高速にすることができる。

【図面の簡単な説明】

【図1】本発明を適用したMMC110の内部構成を示す図である。

【図2】本発明を適用したMMC110のホスト機器220の内部構成、およびホスト機器とMMC110との接続状態を示す図である。

【図3】ICカードチップのコールドリセット時の信号波形を示す図である。

【図4】ICカードチップのウォームリセット時の信号波形を示す図である。

【図5】ICカードチップのICカードコマンド処理時の信号波形を示す図である。

【図6】ICカードチップの非活性化時の信号波形を示す図である。

【図7】ホスト機器によるMMCへのアクセスを示したフローチャートである。

【図8】ICカード制御パラメータとそれに対応するICカードへの処理内容を示す表である。

【図9】ICカードチップに対する第1次ICカード初期化の詳細なフローチャートである。

【図10】ICカードチップに対する第2次ICカード初期化の詳細なフローチャートである。

【図11】非活性状態のICカードチップに対するICカード初期化時の信号波形を示す図である。



【図 1 2】 活性状態の I C カードチップに対する I C カード初期化時の信号波形を示す図である。

【図 1 3】 I C カードチップによるセキュリティ処理の詳細なフローチャートである。

【図 1 4】 セキュリティ処理要求ライトコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。

【図 1 5】 I C カードチップによるセキュリティ処理実行時の信号波形とフラッシュメモリチップアクセスの一例を示す図である。

【図 1 6】 セキュリティ処理結果リードコマンドを処理するときの信号波形とフラッシュメモリチップアクセスを示す図である。

【図 1 7】 インタフェース直通モードにおける MMC 外部端子と I C カードチップ外部端子の対応関係を示す図である。

【図 1 8】 インタフェース直通モードへ移行する処理とインタフェース直通モードから復帰する処理のフローチャートである。

【図 1 9】 インタフェース直通モードへ移行する処理時の信号波形を示す図である。

【図 2 0】 インタフェース直通モードから復帰する処理時の信号波形を示す図である。

【図 2 1】 フラッシュメモリチップの内部構成を示す図である。

【図 2 2】 本発明を適用した MMC の内部構成を簡単に示す図である。

【図 2 3】 本発明を適用した MMC をコンテンツ配信に応用した例を示す図である。

【図 2 4】 本発明を適用した S D カードの内部構成を簡単に示す図である。

【図 2 5】 本発明を適用したメモリースティックの内部構成を簡単に示す図である。

【図 2 6】 本発明の I C カードチップの内部構成を示す図である。

【図 2 7】 並列に処理できるデータリード処理の流れを示した図である。

【図 2 8】 リードコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸にそって示した図である。

【図 2 9】 並列に処理できるデータライト処理の流れを示した図である。

【図 3 0】 ライトコマンドを並列処理する時のコマンドとデータの流れ、処理を時間軸にそって示した図である。

【図 3 1】 並列に処理できるデータを転送しないコマンドの処理を示した図である。

【図 3 2】 並列に処理できるデータを転送しないコマンドの実行する時の処理を時間軸にそって示した図である。

【図 3 3】 並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを示した図である。

【図 3 4】 並列に処理できるデータリード処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。

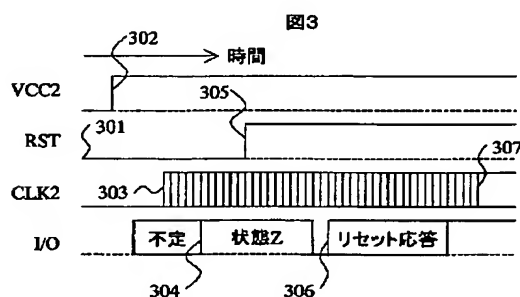
【図 3 5】 並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを示した図である。

【図 3 6】 並列に処理できるデータライト処理とデータ転送を伴わないコマンドの処理の流れを時間軸にそって示した図である。

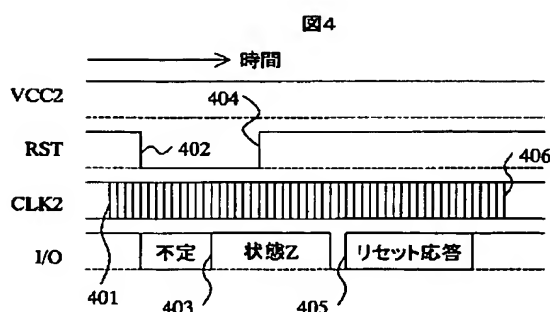
【符号の説明】

1 1 0…MMC、1 2 0…コントローラチップ、1 4 0…MMC 外部端子、1 5 0…I C カードチップ、1 5 1…VCC2 端子、1 5 2…RST 端子、1 5 3…CLK2 端子、1 5 5…GND2 端子、1 5 6…VPP 端子、1 5 7…I/O 端子、2 2 0…ホスト機器、1 4 0 5…ライトコマンド発行、1 9 0 6…モード移行時刻、2 0 0 3…モード復帰時刻。

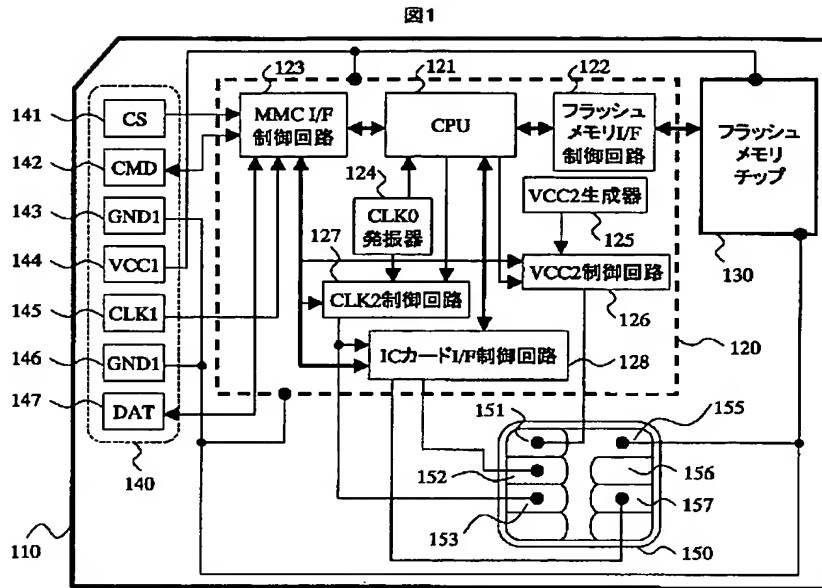
【図 3】



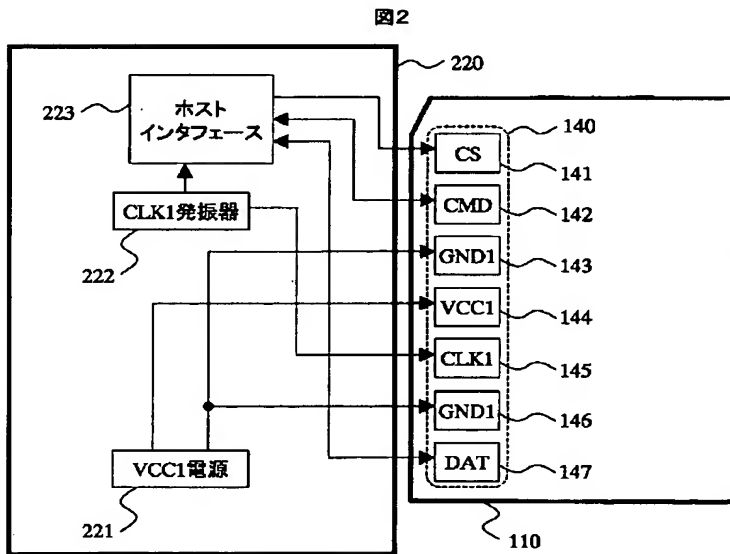
【図 4】



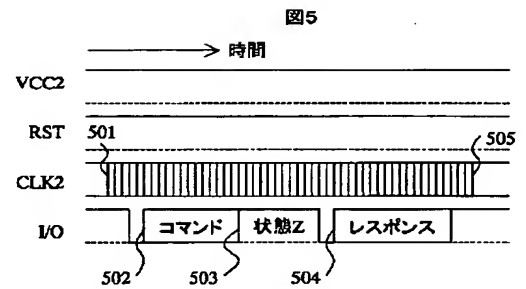
【図 1】



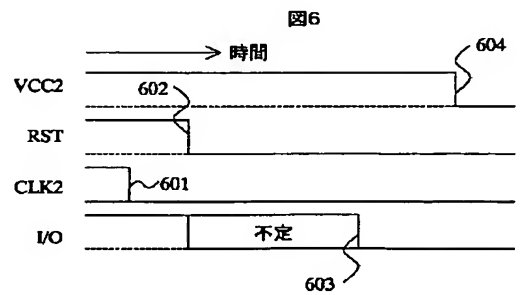
【図 2】



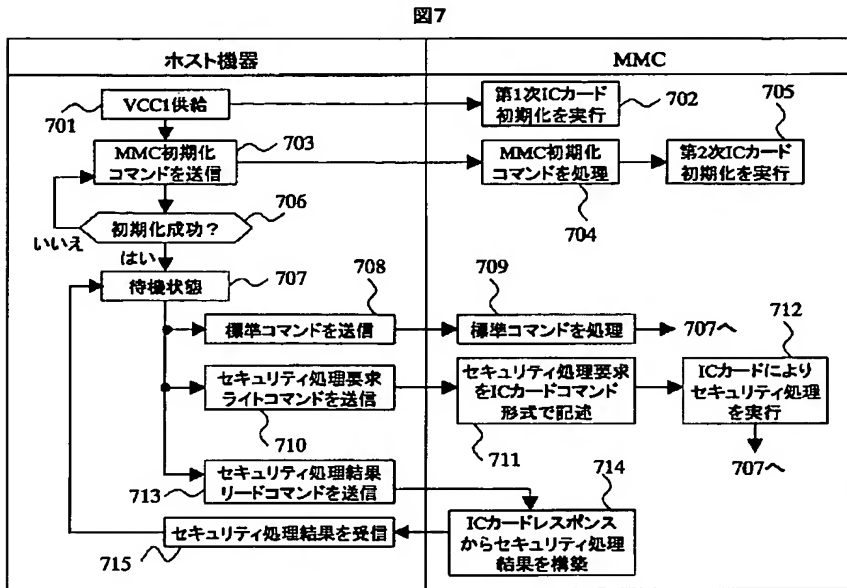
【図 5】



【図 6】



【図 7】



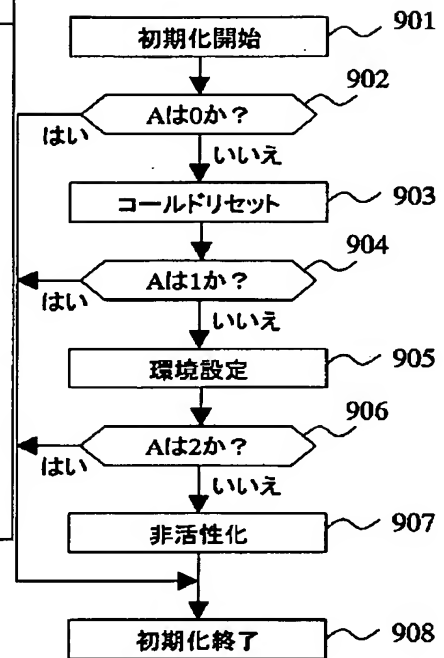
【図 8】

図 8

ICカード制御パラメータ	ICカードに対する処理
A=0	MMCのパワーオン時に、何もしない
A=1	MMCのパワーオン時に、リセット
A=2	MMCのパワーオン時に、リセットと環境設定
A=3	MMCのパワーオン時に、リセットと環境設定し、非活性化
B=0	MMCの初期化時に、何もしない
B=1	C=1 MMCの初期化時に、リセット
	C=2 MMCの初期化時に、リセットと環境設定
	C=3 MMCの初期化時に、リセットと環境設定し、非活性化
B=2	C=2 MMCの初期化時に、環境設定
	C=3 MMCの初期化時に、環境設定し、非活性化
B=3	MMCの初期化時に、活性状態ならば、非活性化
D=0	セキュリティ処理後に、非活性化しない
D=1	セキュリティ処理後に、非活性化する

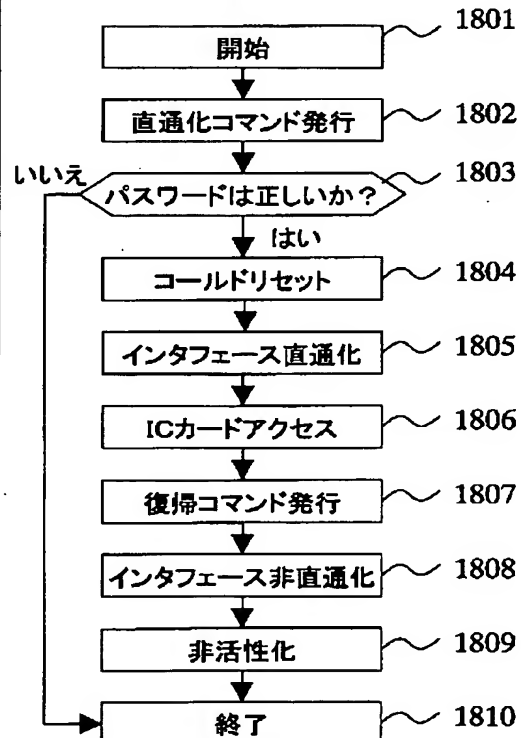
【図 9】

図 9

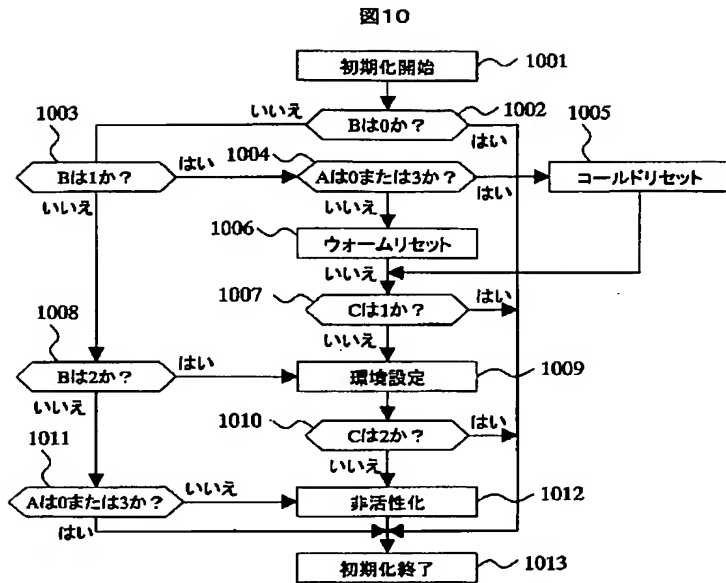


【図 18】

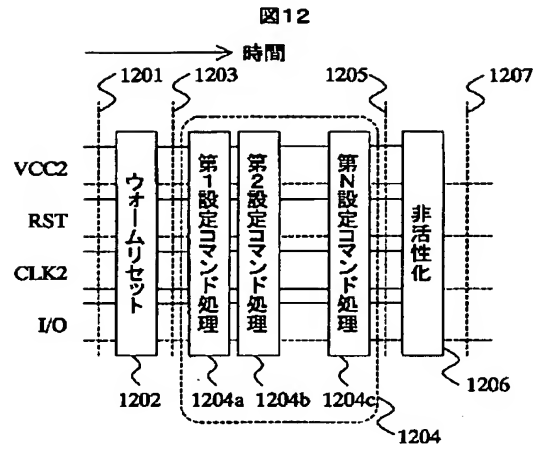
図 18



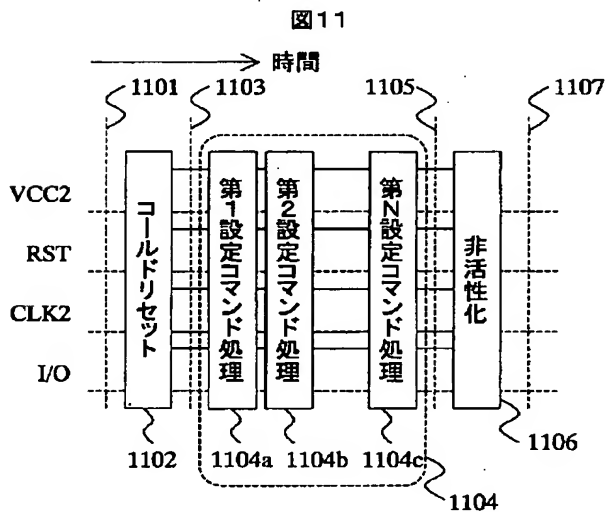
【図 10】



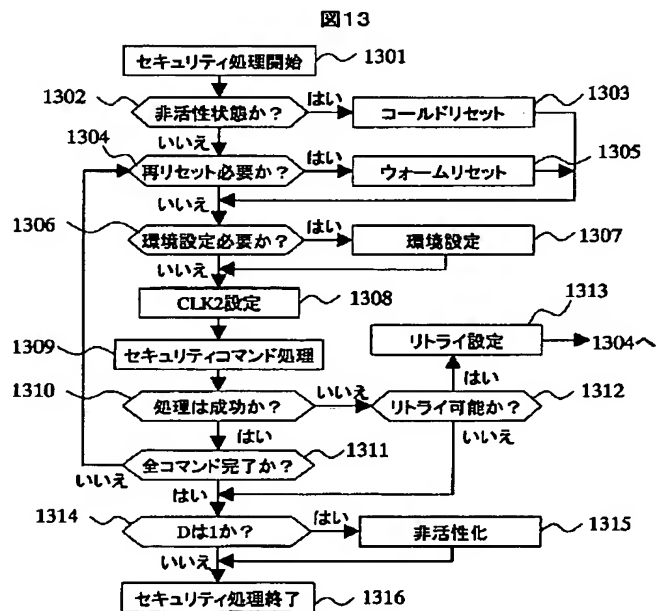
【図 12】



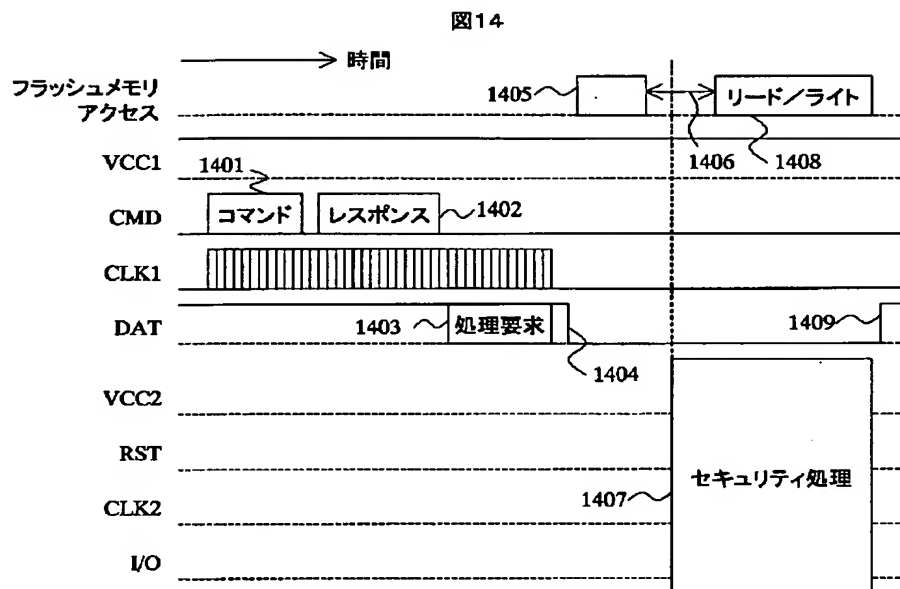
【図 11】



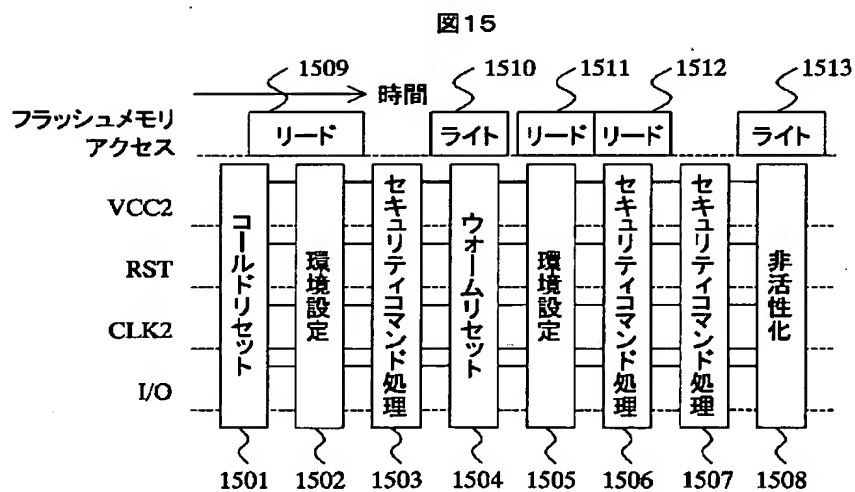
【図 13】



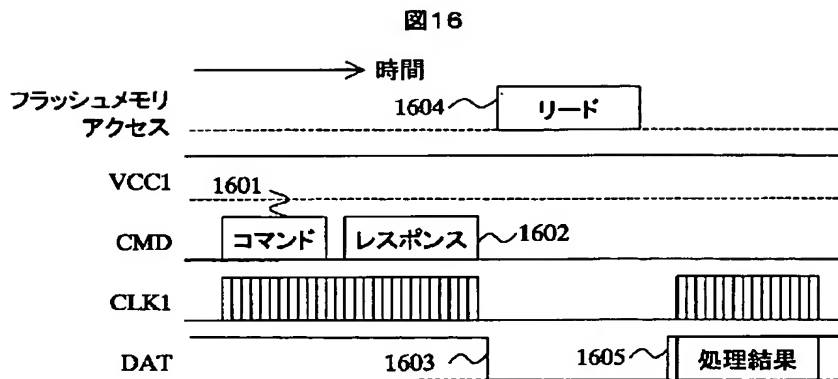
【図 14】



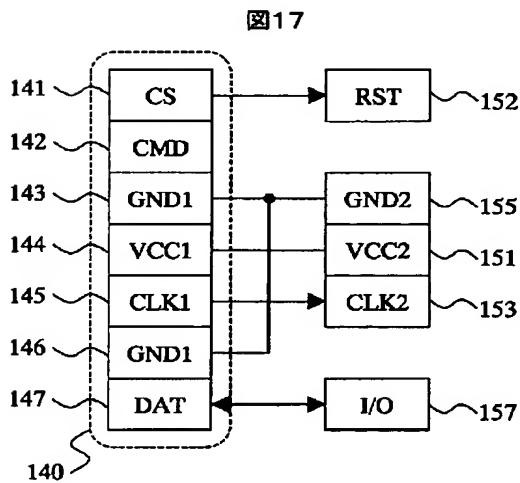
【図 15】



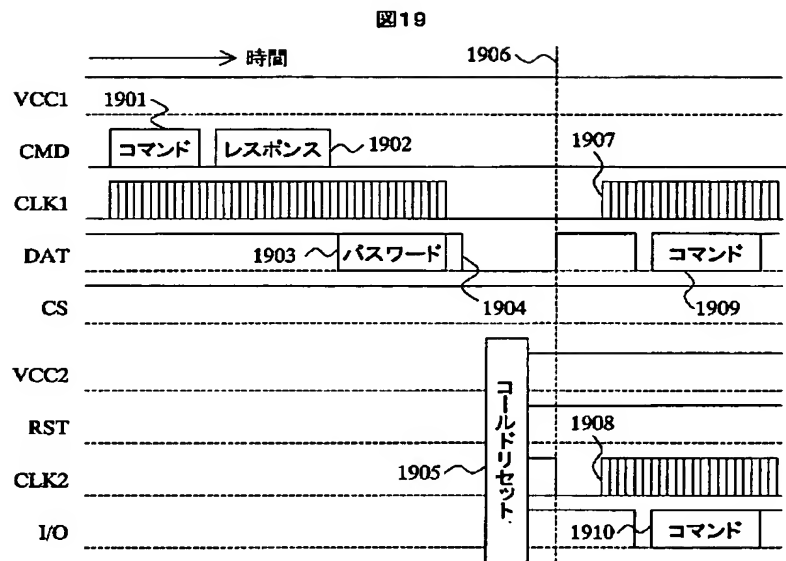
【図 16】



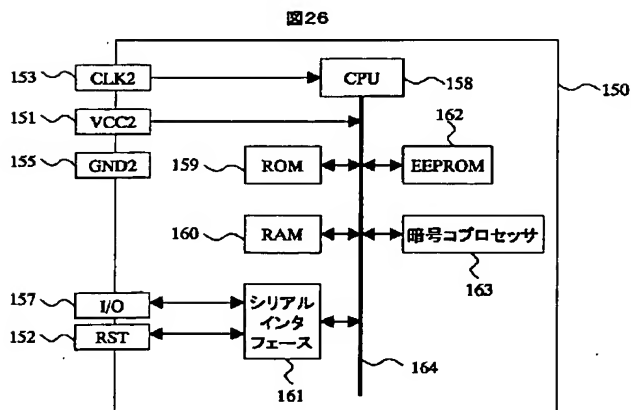
【図 17】



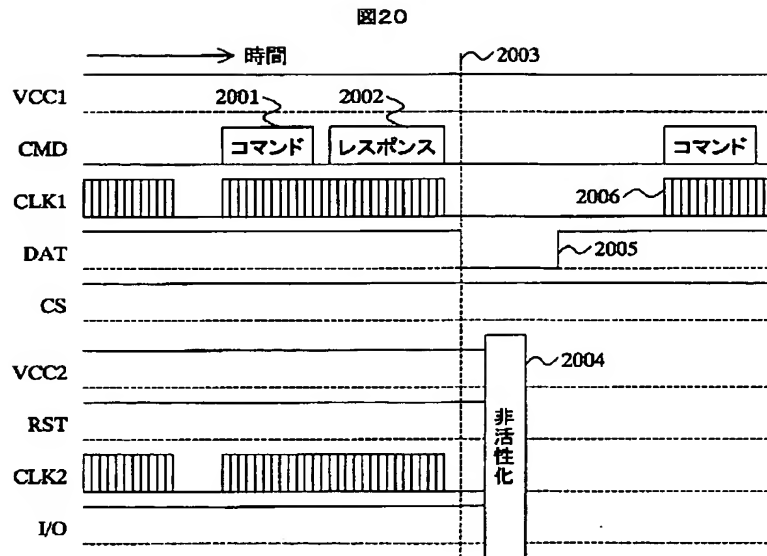
【図 19】



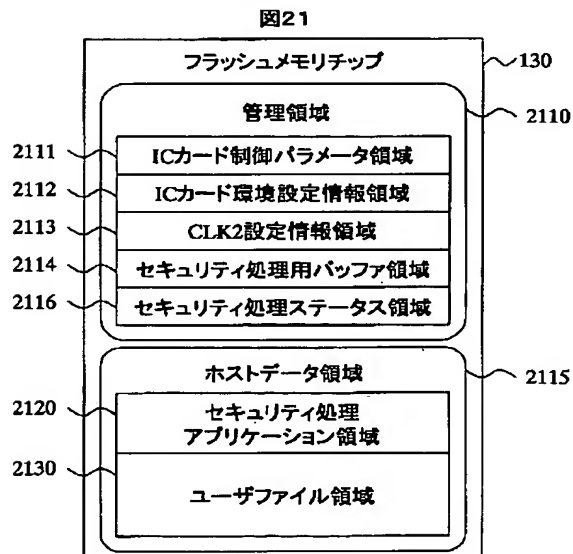
【図 26】



【図 20】



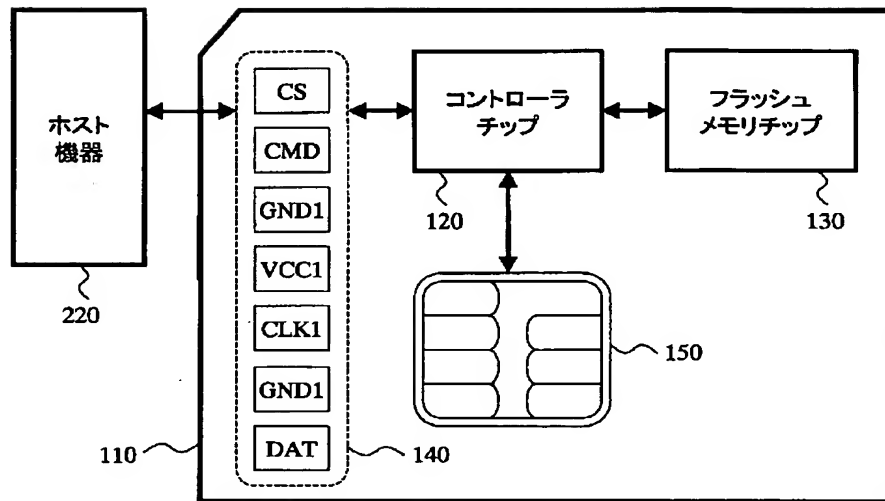
【図 21】





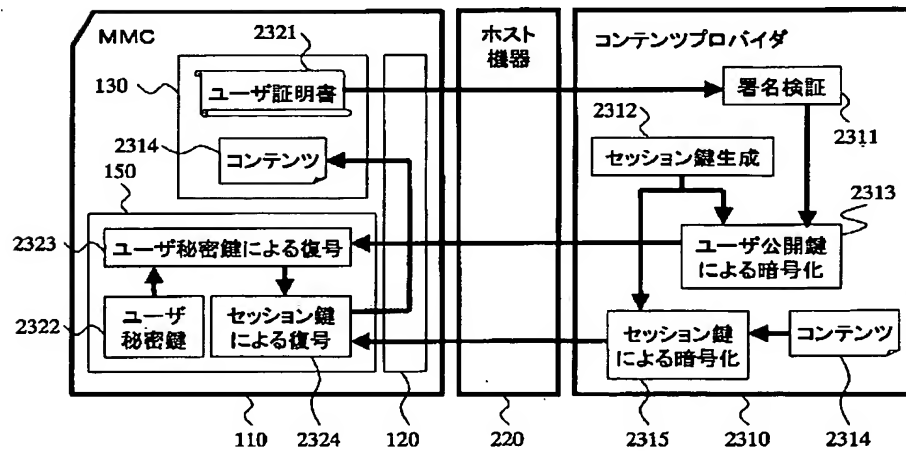
【図 22】

図22



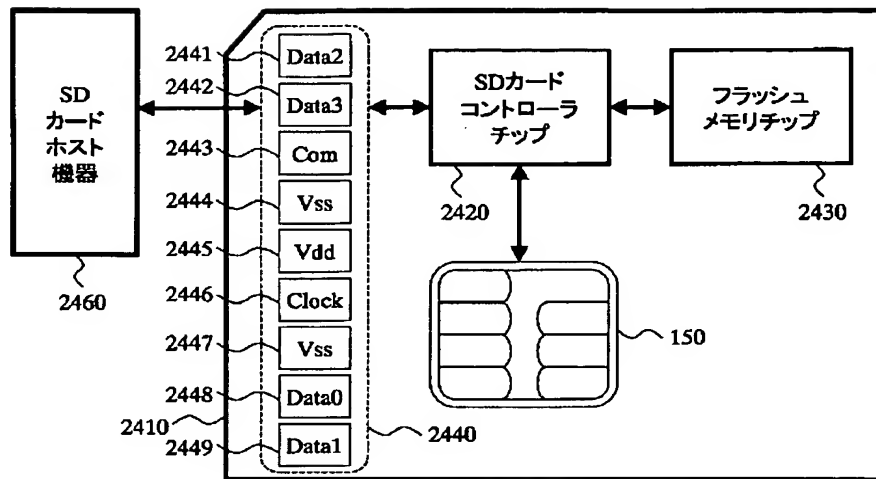
【図 23】

図23



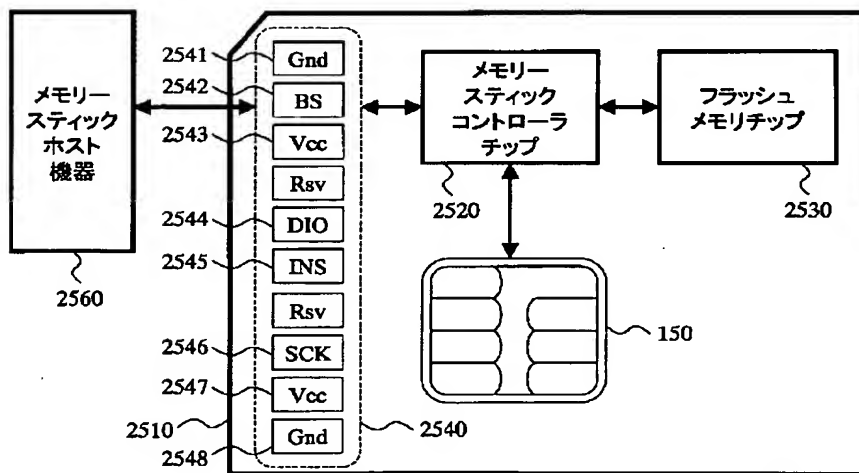
【図 24】

図24

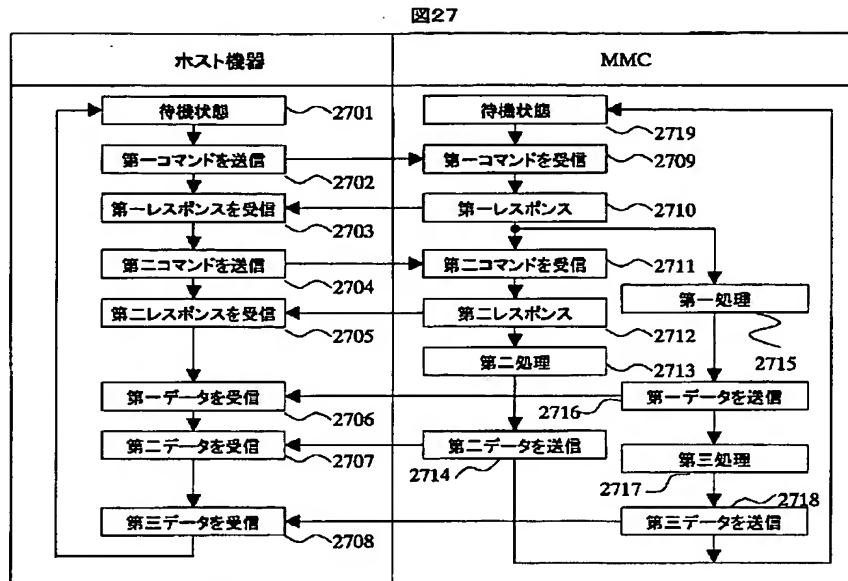


【図 25】

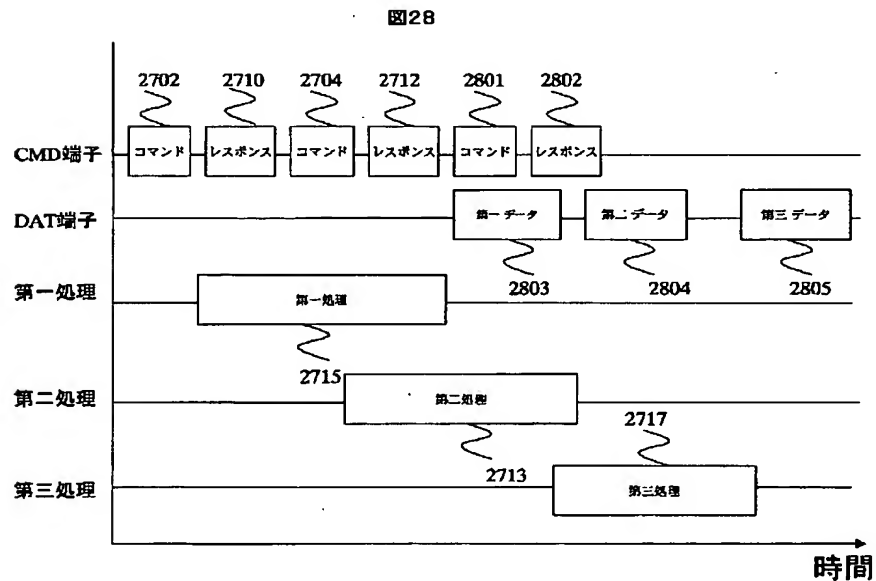
図25



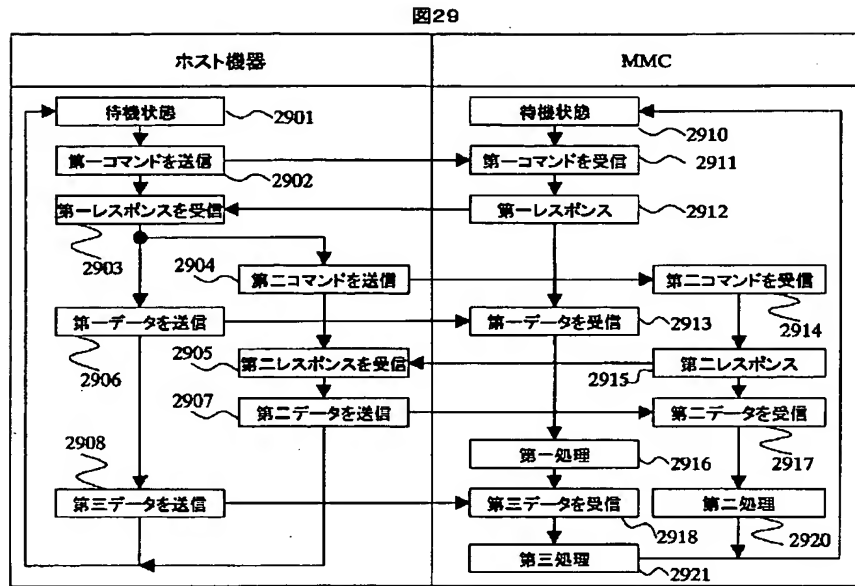
【図 27】



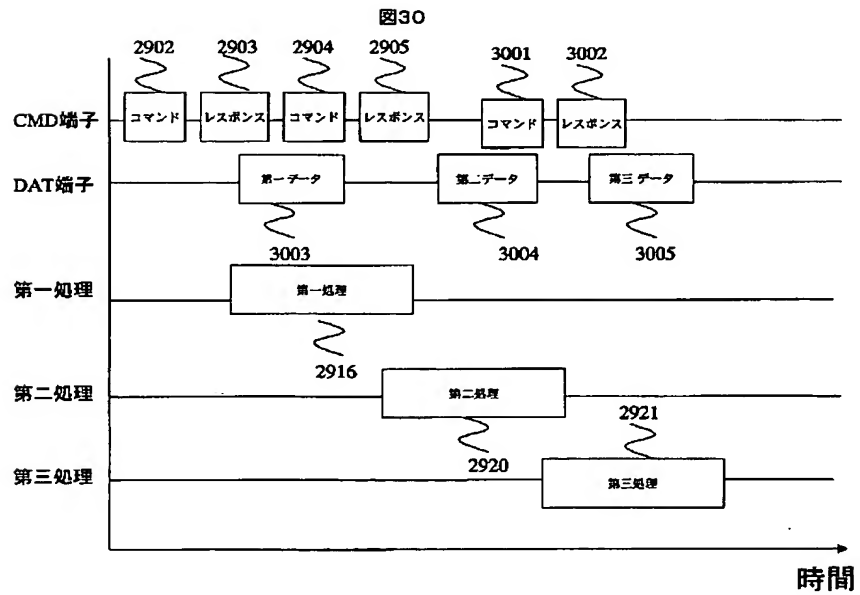
【図 28】



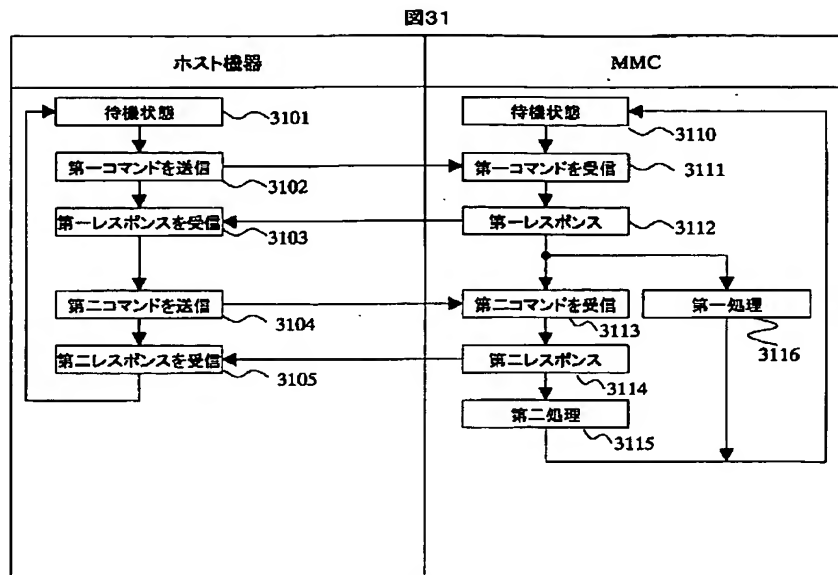
【図 29】



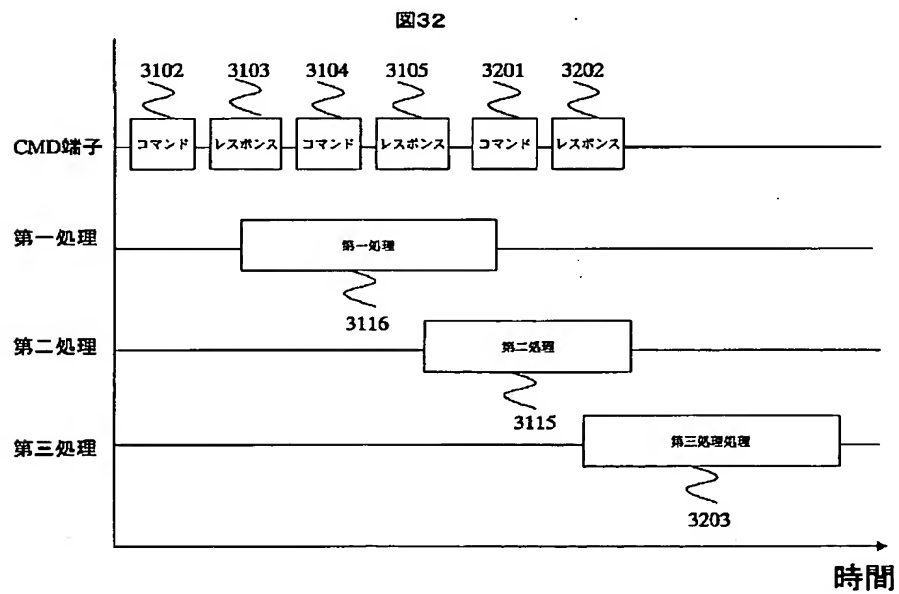
【図 30】



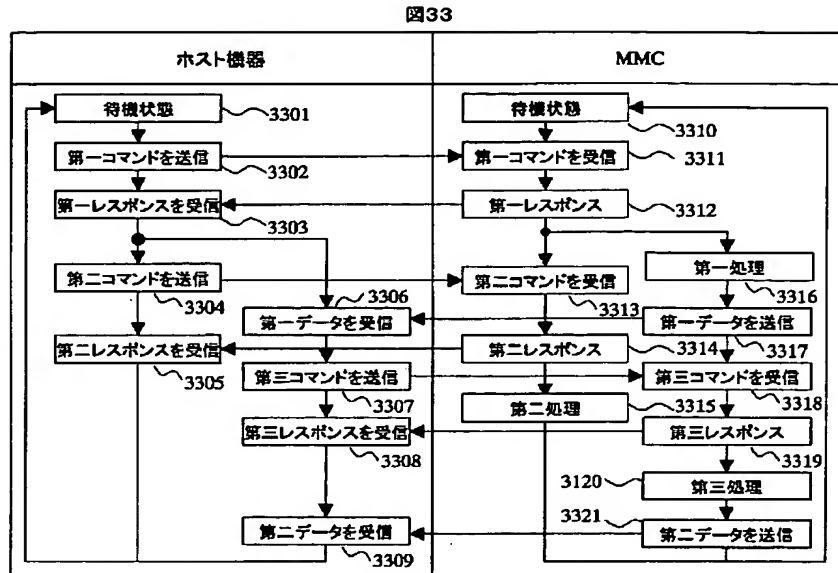
【図 3 1】



【図 3 2】

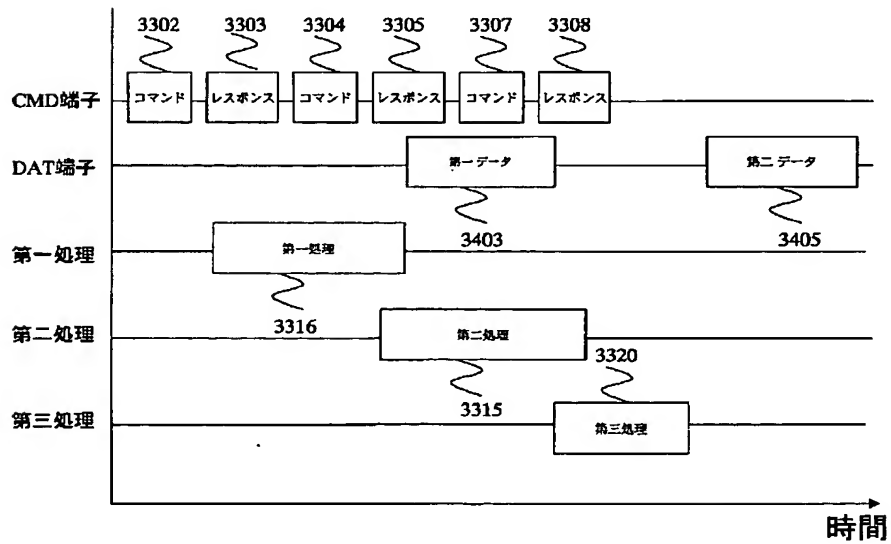


【図 33】

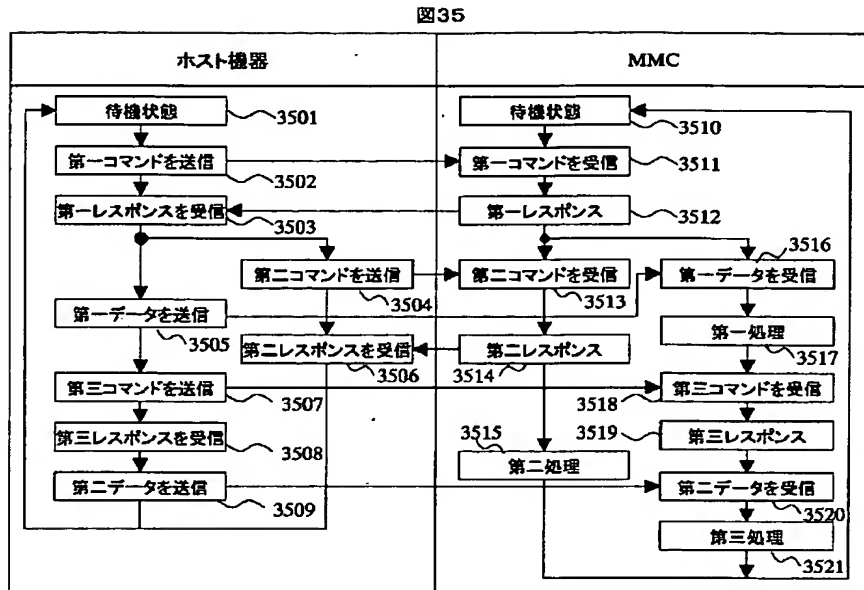


【図 34】

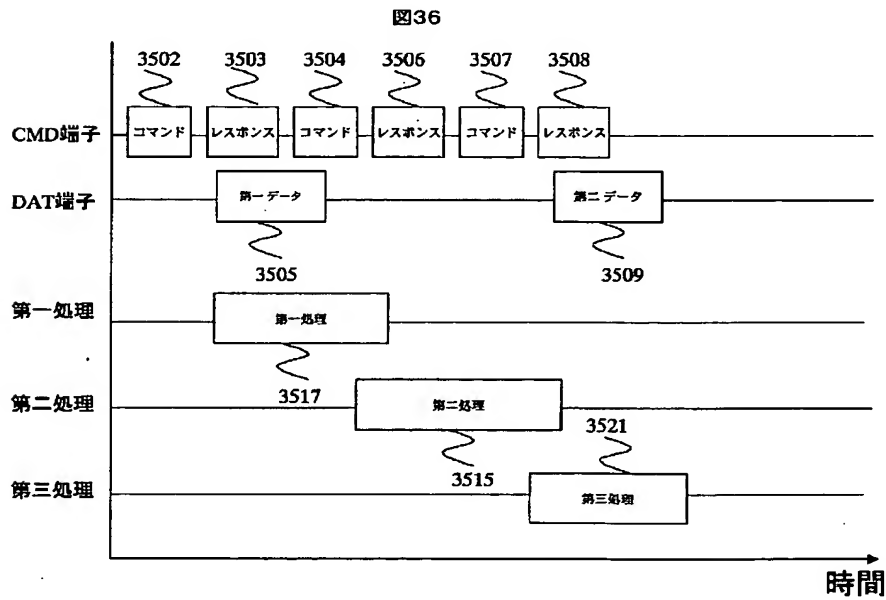
図34



【図 35】



【図 36】



フロントページの続き

(72)発明者 角田 元泰  
神奈川県川崎市麻生区王禅寺1099番地 株  
式会社日立製作所システム開発研究所内  
(72)発明者 水島 永雅  
神奈川県川崎市麻生区王禅寺1099番地 株  
式会社日立製作所システム開発研究所内

(72)発明者 片山 国弘  
東京都小平市上水本町五丁目20番1号 株  
式会社日立製作所半導体グループ内



F ターム(参考) 2C005 MA19 MB02 MB07 NA10 PA18  
PA21 RA22 WA03 WA09  
5B017 AA07 BA06 BA07 CA14  
5B035 AA13 BB09 BC00 CA07 CA11  
CA29